

Nathan Guest (State Bar No. 330167)
nguest@wshblaw.com
WOOD, SMITH, HENNING & BERMAN LLP
 10960 Wilshire Boulevard, 18th Floor
 Los Angeles, California 90024-3804
 Phone: 310-481-7600 ♦ Fax: 310-481-7650

Attorney for Defendant, LIFELONG MEDICAL CARE, a California corporation

**UNITED STATES DISTRICT COURT
 NORTHERN DISTRICT OF CALIFORNIA**

NOEM MARGOLIES, individually and on
 behalf of all others similarly situated

Plaintiffs,

v.

LIFELONG MEDICAL CARE, a California
 corporation, and DOES 1-50, inclusive,,

Defendants.

Case No. _____

**NOTICE OF REMOVAL OF ACTION
 UNDER 28 U.S.C.A. § 1332(d)**

**[DIVERSITY JURISDICTION UNDER
 CLASS ACTION FAIRNESS ACT]**

Superior Court Case No.: RG21113030
 (Alameda County)

LIFELONG MEDICAL CARE, a California
 corporation

Cross-Complainant,

v.

NETGAIN TECHNOLOGY, INC., a
 Minnesota corporation, and ROES 1-50,
 inclusive,

Cross-Defendants.

AND ALL RELATED CROSS-ACTIONS

Action Filed: 9/17/2021
 Cross-Complaint Filed: 11/29/2021

Trial Date: None Set

1 **TO THE CLERK OF THE ABOVE-ENTITLED COURT:**

2 **PLEASE TAKE NOTICE** that pursuant to 28 U.S.C. § 1332(d), and on the grounds set
 3 forth below, Defendant, LIFELONG MEDICAL CARE (“LifeLong”) hereby removes the above-
 4 captioned action, styled *NOEM MARGOLIES, individually and on behalf of all other similarly*
 5 *situated v. LIFELONG MEDICAL CARE, a California Corporation v. NETGAIN TECHNOLOGY,*
 6 *INC., a Minnesota corporation, and ROES 1-50, inclusive*, Case No. RG21113030, from the
 7 Superior Court of the State of California for the County of Alameda to this Court. The factual bases
 8 in support of this Notice of Removal are set forth in further detail below.

9 **I. FACTUAL BACKGROUND**

10 1. On September 17, 2021, Plaintiff Noem Margolies (“Plaintiff”) commenced the
 11 above-referenced action in the Superior Court of the State of California for the County of Alameda
 12 (the “Superior Court”) by filing a Complaint (the “Complaint”) against Defendant, LifeLong,
 13 alleging violations of the California Consumer Privacy Act of 2018, Civil Code §§ 1798.100, et
 14 seq.; California Confidentiality of Medical Information Act (“CMIA”), Civil Code §§ 56, et seq.;
 15 and California Unfair Competition Law, Bus. & Prof. Code §§ 17200, et seq.; as well as causes of
 16 action for breach of contract and negligence. The Complaint, which names only LifeLong, as a
 17 defendant, alleges the foregoing causes of action based on a data security incident that occurred at
 18 Netgain Technology, Inc., a cloud hosting and information technology vendor who provided such
 19 services to LifeLong. A copy of the Complaint, along with its accompanying exhibits, is attached
 20 hereto as **Exhibit 1**.

21 2. Although Plaintiff failed to properly serve the Complaint on LifeLong, LifeLong
 22 executed a statement of service form (the “Service Form”), which was sent to Plaintiff’s counsel on
 23 November 15, 2021. A copy of the Service Form is attached hereto as **Exhibit 2**.

24 3. Following the execution and delivery of the Service Form, LifeLong filed a Cross-
 25 Complaint against Netgain Technology, Inc. (“Netgain”) on November 29, 2021, alleging causes of
 26 action sounding in equitable/implied indemnity; implied contractual indemnity; breach of written
 27 contract; contribution; apportionment of fault; and declaratory relief (the “Cross-Complaint”). The
 28 basis for LifeLong’s Cross-Complaint against Netgain is the above-referenced data security incident

1 complained of in the Plaintiff's Complaint, which was solely due to a breach which occurred at
 2 Netgain. A copy of the Cross-Complaint is attached hereto as **Exhibit 3**.

3 4. An Answer to the Complaint was also filed on December 6, 2021. A copy of the
 4 Answer is attached hereto as **Exhibit 4**.

5 5. Accordingly, the case in its current form is a class action against LifeLong, and a
 6 Cross-Complaint against Netgain seeking contribution and indemnification for any damages
 7 sustained by the putative class (the "Removed Action").

8 6. LifeLong is a non-profit corporation based in California, with fourteen (14)
 9 community health centers that act as safety net providers of medical, dental, and behavioral health
 10 services to communities in and around the San Francisco Bay Area.

11 7. Netgain is a Delaware corporation, with its principal headquarters located in St.
 12 Cloud, Minnesota, that provides specialized cloud hosting and information technology services and
 13 solutions. Netgain's clients include healthcare providers across the country, from California to
 14 South Carolina.

15 II. VENUE

16 8. Venue is proper in this Court pursuant to 28 U.S.C. § 1446 as the United States
 17 District Court for the Northern District of California embraces the state court in the County of
 18 Alameda, California, in which Plaintiff filed his state court Complaint.

19 9. Specifically, venue in the San Francisco or Oakland Division of the Northern District
 20 of California is proper pursuant to Local Rule 3-2(d).

21 III. DIVERSITY JURISDICTION UNDER CAFA

22 10. Federal district courts have original jurisdiction over "class actions" in which (i) the
 23 matter in controversy exceeds the sum or value of \$5,000,000, exclusive of interests and costs, and
 24 (ii) any member of a class of plaintiff is a citizen of a State different from any defendant. 28 U.S.C.
 25 § 1332(d)(2).

26 11. Section 1332(d)(1)(B) defines "class action" as any civil action filed under Fed. R.
 27 Civ. P. Rule 23 or similar state statute or rule of judicial procedure authorizing an action to be
 28 brought by one or more representative persons as a class action. 28 U.S.C. § 1332(d)(1)(B).

12. Further, under the Class Action Fairness Act (CAFA), a federal court may exercise subject matter jurisdiction over a class action where (1) the parties are minimally diverse; (2) the proposed class has at least 100 members; and (3) the amount in controversy exceeds \$5,000,000. 28 U.S.C. § 1332(d); Prado v. Dart Container Corporation of California, 373 F.Supp.3d 1281, 1285-86 (N.D. Cal. 2019); Kuxhausen v. BMW Fin. Servs. NA LLC, 707 F.3d 1136, 1139 (9th Cir. 2013).

13. The Class Action Fairness Act also amended 28 U.S.C. § 1453 such that any defendant may remove to federal court, regardless of whether it is a citizen of the State in which the action is brought, and that the removing defendant does not need the consent of all defendants in order to effectuate removal to federal court. 28 U.S.C. § 1453(b); Abrego v. The Dow Chemical Co., 443 F.3d 676, 681 (9th Cir. 2006).

14. As for the timeliness of removal, Section 1446(b)(3) sets forth that, where the case stated by the initial pleading is not removable, a notice of removal may be filed within 30 days from when “it may first be ascertained that the case is one which is or has become removable.” 28 U.S.C. § 1446(b)(3); Jordan v. Nationstar Mortg. LLC, 781 F.3d 1178, 1183-84 (9th Cir. 2015). In this regard, the case may be removed within 30 days from when the case becomes removable, even if an earlier pleading, document, motion, order, or other paper revealed an alternative basis for federal jurisdiction. Id. at 1180; Kenny v. Wal-Mart Stores, Inc., 881 F.3d 786, 791 (9th Cir. 2018).

IV. GROUNDS FOR REMOVAL

15. Upon the filing of LifeLong’s Cross-Complaint against Netgain, the Removed Action satisfied all requirements for removal under the Class Action Fairness Act, and this Notice of Removal has been timely filed with the Northern District. Pursuant to CAFA, the filing of this Notice of Removal by LifeLong is permissible, notwithstanding LifeLong’s residence as a California corporation, where Plaintiff’s state court action was filed. 28 U.S.C. § 1453(b).

16. First, the Removed Action qualifies as a “class action” as defined by Section 1332(d)(1)(B), as Plaintiff’s Complaint has been filed by “Noem Margolies, individually and on behalf of all other similarly situated” and specifically states that it is being filed as a class action pursuant to Cal. Code Civ. Proc. § 382. See Complaint, at ¶ 7-9. In this regard, the Removed Action is a lawsuit pursuant to State statute authorizing an action to be brought by one or more persons as

1 representative of a class action.

2 17. Further, the parties to the lawsuit meet the minimal diversity requirement set forth in
3 Section 1332(d)(2)(A), as Plaintiff Noem Margolies and Defendant, LifeLong, are both citizens of
4 the state of California, whereas Netgain is a Delaware corporation, with a principal place of business
5 in Minnesota. 28 U.S.C. § 1332(d)(2)(A); See Cross-Complaint, at ¶ 3.

6 18. The proposed class also contains far more than the requisite 100 members, as
7 Plaintiff's Complaint alleges a putative class of 115,448. As set forth in the Complaint, this number
8 derives from the notification submitted by LifeLong to the U.S. Department of Health and Human
9 Services' (HHS) regarding the data security incident at Netgain. See Complaint, at ¶ 56.

10 19. Likewise, the amount in controversy is well above the \$5,000,000 minimum given
11 both the size of the proposed class, and the statutory damages claimed by Plaintiff in the Complaint.
12 In particular, Plaintiff alleges violations of the CCPA, which carry potential statutory damages of
13 \$100 to \$750 per Plaintiff. See Complaint, at ¶ 114; see also Cal. Civ. Code § 1798.150(a)(1)(A).

14 20. Plaintiff also alleges violations of the CMIA, which carry statutory damages of
15 \$1,000 per violation, per Plaintiff, as well as potential punitive damages of \$3,000 per Plaintiff. See
16 Complaint, at ¶ 132; see also Cal. Civ. Code §§ 56.36(b)(1), 56.35.

17 21. Accordingly, the \$5,000,000 threshold set forth in Section 1332(d)(2) is clearly met
18 by the Removed Action, given the proposed class size of 115,448. In this regard, Plaintiff alleges
19 damages which, at a minimum, come out to \$1,100 per person (\$100 under the CCPA and \$1,000
20 under the CMIA), constituting a minimum amount in controversy which well exceeds \$5,000,000.

21 22. Finally, this Notice of Removal is being filed in a timely manner, as the Removed
22 Action first became removable upon the filing of LifeLong's Cross-Complaint impleading Netgain
23 on November 29, 2021, given that Netgain is not domiciled in California and does not have its
24 principal place of business in California. Prior to the filing of the Cross-Complaint, the only parties
25 to the lawsuit were California citizens, which would have been insufficient for purposes of meeting
26 minimal diversity under Section 1332.

27 ///

28 ///

23. As this Notice of Removal is being filed within 30 days of the filing of the Cross-Complaint, removal has been effectuated in a timely manner. 28 U.S.C. § 1446(b)(3).

DATED: December 29, 2021

WOOD, SMITH, HENNING & BERMAN LLP

By:



NATHAN GUEST

Attorneys for Defendant, LIFELONG MEDICAL
CARE, a California corporation

WOOD, SMITH, HENNING & BERMAN LLP
Attorneys at Law
10960 WILSHIRE BOULEVARD, 18TH FLOOR
LOS ANGELES, CALIFORNIA 90024-3804
TELEPHONE 310-481-7600 ♦ FAX 310-481-7650

EXHIBIT "1"




23127821

KAZEROUNI LAW GROUP, APC
 Abbas Kazerounian, Esq. (SBN 249203)
 ak@kazlg.com
 Mona Amini (SBN 296829)
 mona@kazlg.com
 245 Fischer Avenue, Unit D1
 Costa Mesa, California 92626
 Telephone: (800) 400-6808
 Facsimile: (800) 520-5523

FILED
ALAMEDA COUNTY

SEP 17 2021

CLERK OF THE SUPERIOR COURT
 By 
 JAMIE THOMAS, Deputy

Attorneys for Plaintiff and the Proposed Class

SUPERIOR COURT OF THE STATE OF CALIFORNIA
FOR THE COUNTY OF ALAMEDA – COMPLEX CIVIL

NOEM MARGOLIES, individually and on behalf
 of all others similarly situated,

Plaintiff,

vs.

LIFELONG MEDICAL CARE, a California
 corporation; and DOES 1-50, inclusive,

Defendant(s).

Case No.: **R021113030**

CLASS ACTION COMPLAINT FOR
 VIOLATIONS OF:

1. CALIFORNIA CONSUMER PRIVACY ACT OF 2018, CAL. CIV. CODE §§ 1798.100, *et seq.*;
2. CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CAL. CIV. CODE §§ 56, *et seq.*;
3. CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE §§ 17200, *et seq.*;
4. BREACH OF CONTRACT; and
5. NEGLIGENCE

DEMAND FOR JURY TRIAL

//

//

//

//

//

//

//



1 Plaintiff Noem Margolies (“Plaintiff”), individually and on behalf of the general public and
 2 all others similarly situated (the “Class members”), by and through Plaintiff’s attorneys, upon
 3 personal knowledge as to facts pertaining to themselves and on information and belief as to all other
 4 matters, bring this class action against Defendant Lifelong Medical Care and DOES 1-50, inclusive
 5 (“Defendant”), and alleges as follows:

6 **NATURE OF THE CASE**

7 1. This is a data breach class action arising out of Defendant’s failure to implement and
 8 maintain reasonable security practices to protect consumers’ sensitive personal information.
 9 Defendant is a healthcare provider that has served patients for over 45 years.¹ For its business
 10 purposes, Defendant obtains, stores, and transmits personally identifiable information (“PII”) and
 11 protected health information (“PHI”) from patients like Plaintiff, including but not limited to patients’
 12 names, addresses, social security numbers, dates of birth, patient cardholder numbers, telephone
 13 numbers, healthcare account numbers and balances, and treatment/diagnosis information.

14 2. On November 24, 2020, Netgain Technology, LLC (“Netgain”), a third-party vendor
 15 that provided IT services to Defendant, discovered anomalous network activity and determined it was
 16 a victim of a ransomware attack. On February 25, 2021, Netgain’s investigation determined that
 17 certain files were accessed and/or acquired without authorization.

18 3. Thereafter, Defendant conducted its own investigation, and during the investigation,
 19 and on August 9, 2021, Defendant determined that unauthorized users had accessed and/or acquired
 20 certain patients’ PII and PHI from Netgain’s network, including individuals’ full names, social
 21 security numbers, dates of birth, patient cardholder numbers, and/or treatment/diagnosis information
 22 (the “Data Breach”). Although the exact number of affected patients is presently unknown, based
 23 upon information and belief at least 115,448 patients have been affected by the Data Breach. The
 24 Data Breach occurred on or around November 24, 2020. However, Defendant only provided notice
 25 to Plaintiff and its other patients impacted by the Data Breach on or around August 24, 2021.
 26
 27
 28

¹ <https://lifelongmedical.org/about-us/>



4. Although Defendant knew about the Data Breach and that sensitive patient information was in the hands of malicious actors, it waited until on or around August 24, 2021, to send Plaintiff and other similarly situated patients letters regarding the Data Breach. Defendant's notice to patients was misleading and inadequate as the notice did not explain the *nine-month delay* between the discovery of the Data Breach and notifying affected patients.

5. This action seeks to remedy Defendant's failure to safeguard Plaintiff and the Class' PII and PHI. Plaintiff brings this action on behalf of Plaintiff individually and all other persons impacted by the Data Breach.

6. As set forth in the Prayer for Relief, among other things, Plaintiff seeks, for themselves and the Class injunctive relief, including public injunctive relief, and actual damages.

VENUE AND JURISDICTION

7. This Court has jurisdiction over this action pursuant to Cal. Code Civ. Proc. § 410.10 and Cal. Bus. & Prof. Code §§ 17203-17204, 17604. This action is brought as a class action on behalf of Plaintiff and the Class members pursuant to Cal. Code Civ. Proc. § 382.

8. This Court has personal jurisdiction over Defendant because Defendant regularly conducts business in California and is headquartered in Berkeley, California.

9. Venue is proper in this Court pursuant to Cal. Code Civ. Proc. § 395 and § 395.5 because Defendant regularly conducts business in the State of California, Defendant is headquartered in Berkeley, California, and the unlawful acts or omissions giving rise to this action also occurred or arose in this county.

PARTIES

10. At all relevant times, Plaintiff resided in the State of California.

11. At all relevant times, Defendant conducted business in the State of California.

12. Plaintiff provided PII/PHI to Defendant, and Defendant collected and maintained certain PII/PHI related to Plaintiff, including but not limited to Plaintiff's name, address, social security number, date of birth, patient cardholder number, and medical treatment/diagnosis information. On August 24, 2021, Plaintiff was notified that Plaintiff's PII/PHI was accessed, viewed, and/or acquired by unauthorized individuals through the Data Breach.



13. Defendant sent Plaintiff a letter dated August 24, 2021, with the title, “*IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY*” (the “Letter”). The Letter notified Plaintiff and similarly situated persons that as a result of the Data Breach a malicious actor had gained unauthorized access to certain PII/PHI in Netgain’s network containing individuals’ PII and PHI, including: full name, social security number, date of birth, patient cardholder numbers, and treatment/diagnosis information. No details were provided regarding the details of the ransomware attack, who stole the information, whether a ransom was paid, if Plaintiff and the Class members’ PII/PHI was recovered, or why there was a significant delay in Defendant notifying Plaintiff and other affected patients.

14. As a result of Defendant’s failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information it collected, maintained, and stored on its servers, network, and/or email system, Plaintiff’s PII/PHI was accessed, viewed, exfiltrated, stolen and/or otherwise disclosed to unauthorized persons in the Data Breach.

15. Defendant is a California company formed under the laws of the State of California with a headquarters located at 2344 6th Street, Berkeley, California 94710. Defendant is a medical provider that offers medical, dental, and social services.

16. Plaintiff is unaware of the true names and capacities of the Defendant sued herein as DOES 1 through 50, inclusive, and therefore sue this Defendant by such fictitious names pursuant to Cal. Civ. Proc. Code § 474. Plaintiff is informed and believes, and based thereon, alleges that Defendant designated herein is legally responsible in some manner for the unlawful acts and occurrences complained of herein, whether such acts were committed intentionally, negligently, recklessly, or otherwise, and Defendant thereby proximately caused the injuries and damages to Plaintiff and the Class members as herein alleged. Plaintiff will seek leave of Court to amend this complaint to reflect the true names and capacities of Defendant when they have been ascertained and become known.

17. The agents, servants and/or employees of Defendant and each of them acting on behalf of Defendant acted within the course and scope of his, her or its authority as the agent, servant and/or employee of Defendant, and personally participated in the conduct alleged herein on behalf of Defendant with respect to the conduct alleged herein. Consequently, the acts of each Defendant are

1 legally attributable to the other Defendants and all Defendants are jointly and severally liable to
 2 Plaintiff and other similarly situated individuals, for the loss sustained as a proximate result of the
 3 conduct of the Defendants' agents, servants and/or employees.

4 **FACTUAL ALLEGATIONS**

5 ***PII/PHI Is a Valuable Property Right that Must Be Protected***

6 18. The California Constitution guarantees every Californian a right to privacy. PII/PHI is
 7 a recognized valuable property right.² California has repeatedly recognized this property right, most
 8 recently with the passage of the California Consumer Privacy Act of 2018.

9 19. In a Federal Trade Commission ("FTC") roundtable presentation, former
 10 Commissioner, Pamela Jones Harbour, underscored the property value attributed to PII by observing:

11 Most consumers cannot begin to comprehend the types and amount of
 12 information collected by businesses, or why their information may be
 13 commercially valuable. Data is currency. The larger the data set, the greater
 14 potential for analysis – and profit.³

15 20. The value of PII as a commodity is measurable. "PII, which companies obtain at little
 16 cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional
 17 financial assets."⁴ It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals
 18 often trade it on the "cyber black-market" for several years.

19 21. Companies recognize PII as an extremely valuable commodity akin to a form of
 20 personal property. For example, Symantec Corporation's Norton brand has created a software
 21 application that values a person's identity on the black market.⁵

22 22. As a result of its real value and the recent large-scale data breaches, identity thieves
 23 and cyber criminals openly post credit card numbers, Social Security numbers, PII and other sensitive

24 ² See John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable*
 25 *Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *2 (2009)
 26 ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level
 27 comparable to the value of traditional financial assets.") (citations omitted).

28 ³ FTC, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC
 Exploring Privacy Roundtable) (Dec. 7, 2009), <https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable>.

⁴ See Soma, *Corporate Privacy Trend*, *supra*.

⁵ Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessmenttool.html.

information directly on various illicit Internet websites making the information publicly available for other criminals to take and use. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims. In one study, researchers found hundreds of websites displaying stolen PII and other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism – the "Safe Browsing list."

23. PHI is particularly valuable. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers and bank account information, complete with account and routing numbers, can fetch up to \$1,200 to \$1,300 each on the black market.⁶ According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen social security or credit card number.⁷

24. Recognizing the high value that consumers place on their PII/PHI, some companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share – and who ultimately receives that information. By making the transaction transparent, consumers will make a profit from the surrender of their PII/PHI.⁸ This business has created a new market for the sale and purchase of this valuable data.⁹

25. Consumers place a high value not only on their PII/PHI, but also on the privacy of that data. Researchers shed light on how much consumers value their data privacy – and the amount is

⁶ Adam Greenberg, *Health Insurance Credentials Fetch High Prices in the Online Black Market* (July 16, 2013), available at <https://www.scmagazine.com/home/security-news/health-insurance-credentials-fetch-high-prices-in-the-online-black-market/>.

⁷ Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014) available at <https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf>.

⁸ Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010) available at <https://www.nytimes.com/2010/07/18/business/18unboxed.html>.

⁹ See Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011) available at <https://www.wsj.com/articles/SB10001424052748703529004576160764037920274>.

considerable. Indeed, studies confirm that “when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites.”¹⁰

26. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their PII between \$11.33 and \$16.58 per website.¹¹

27. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers’ PII/PHI has thus deprived that consumer of the full monetary value of the consumer’s transaction with the company.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

28. A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. As more consumers rely on the internet and apps on their phone and other devices to conduct every-day transactions, data breaches are becoming increasingly more harmful.

29. Theft or breach of PII/PHI is serious. The California Attorney General recognizes that “[f]oundational” to every Californian’s constitutional right to privacy is “information security: if companies collect consumers’ personal data, they have a duty to secure it. An organization cannot protect people’s privacy without being able to secure their data from unauthorized access.”¹²

30. The United States Government Accountability Office noted in a June 2007 report on Data Breaches (“GAO Report”) that identity thieves use PII to take over existing financial accounts, open new financial accounts, receive government benefits and incur charges and credit in a person’s name.¹³ As the GAO Report states, this type of identity theft is so harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim’s credit rating.

¹⁰ Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study* *Information Systems Research* 22(2) 254, 254 (June 2011), available at https://www.jstor.org/stable/23015560?seq=1#page_scan_tab_contents.

¹¹ II–Horn, Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, available at <https://ideas.repec.org/p/wpa/wuwpio/0304001.html>.

¹² California Data Breach Report, Kamala D. Harris, Attorney General, California Department of Justice, February 2016.

¹³ See GAO, GAO Report 9 (2007), available at <http://www.gao.gov/new.items/d07737.pdf>.

31. In addition, the GAO Report states that victims of identity theft will face “substantial costs and inconveniences repairing damage to their credit records ... [and their] good name.” According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.¹⁴

32. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.¹⁵ According to Experian, “[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it” to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver license or ID; use the victim’s information in the event of arrest or court action.¹⁶

33. According to the IBM and Ponemon Institute’s 2019 “Cost of a Data Breach” report, the average cost of a data breach per consumer was \$150 per record.¹⁷ Other estimates have placed the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity theft – a common result of data breaches – was \$298 dollars.¹⁸ And in 2019, Javelin Strategy &

¹⁴ See FTC Identity Theft Website: <https://www.consumer.ftc.gov/features/feature-0014-identity-theft>.

¹⁵ The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” 16 C.F.R. § 603.2. The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.” *Id.*

¹⁶ See Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 7, 2017), available at <https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/>.

¹⁷ Brook, *What’s the Cost of a Data Breach in 2019*, *supra*.

¹⁸ Norton By Symantec, 2013 Norton Report 8 (2013), available at https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf.

1 Research compiled consumer complaints from the FTC and indicated that the median out-of-pocket
2 cost to consumers for identity theft was \$375.¹⁹

3 34. The consequences can be even more serious when the hack includes taking PHI. Data
4 breaches involving medical information “typically leave[] a trail of falsified information in medical
5 records that can plague victims’ medical and financial lives for years.”²⁰ It “is also more difficult to
6 detect, taking almost twice as long as normal identity theft.”²¹ “A thief may use your name or health
7 insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider,
8 or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and
9 payment records, and credit report may be affected.”²²

10 35. Further, medical data is more valuable than other commonly available personal data.
11 “While a stolen credit card number might be sold for just a few cents, medical files can be worth as
12 much as \$1,000 each” or more.²³

13 36. A report published by the World Privacy Form and presented at the U.S. FTC
14 Workshop on Informational Injury describes what medical identity theft victims may experience:

- 15 • Changes to their health care records, most often the addition of falsified information,
16 through improper billing activity or activity by imposters. These changes can affect
17 the healthcare a person receives if the errors are not caught and corrected.
- 18 • Significant bills for medical goods and services not sought nor received.
- 19 • Issues with insurance, co-pays, and insurance caps.
- 20 • Long-term credit problems based on problems with debt collectors reporting debt due
21 to identity theft.

22 ¹⁹ Facts + Statistics: *Identity Theft and Cybercrime*, Insurance Information Institute, available
23 at <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (citing the Javelin
report).

24 ²⁰ Pam Dixon, et al., *The Geography of Medical Identity Theft* (Dec. 12, 2017),
https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf.

25 ²¹ See FBI CYBER DIVISION, (U) HEALTH CARE SYSTEMS AND MEDICAL DEVICES AT RISK FOR
26 INCREASED CYBER INTRUSIONS FOR FINANCIAL GAIN 2 (2014), available at
<https://publicintelligence.net/fbi-health-care-cyber-intrusions/> (FBI, April 8, 2014).

27 ²² See Federal Trade Commission, *Medical Identity Theft*, available at
<http://www.consumer.ftc.gov/articles/0171-medical-identity-theft>.

28 ²³ Brian O’Connor, *Healthcare Data Breach: What to Know About Them and What to Do After One*, Experian (June 14, 2018), <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/>.

- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.

37. A person whose PII/PHI has been compromised may not see any signs of identity theft for years. According to the GAO Report:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

38. For example, in 2012, hackers gained access to LinkedIn's users' passwords. However, it was not until May 2016, four years after the breach, that hackers released the stolen email and password combinations.²⁴

39. It is within this context that Plaintiff and over 115,000 of Defendant's patients face imminent risk of identity theft and must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken, accessed, and viewed by unauthorized persons willing and able to use the information for any number of improper purposes and scams, including making the information available for sale on the dark web or the black market.

//

//

//

²⁴ See Cory Scott, *Protecting Our Members*, LINKEDIN (May 18, 2016), available at <https://blog.linkedin.com/2016/05/18/protecting-our-members>.

Defendant's Business

40. Defendant is a healthcare provider that provides medical, dental, and social services to its patients.

41. When Plaintiff and similarly situated patients received medical treatment from Defendant, they are required to provide Defendant with certain personal information. This personal information includes the patient's name, Social Security number, date of birth, patient cardholder number, insurance information, and other medical information related to their medical condition, diagnosis, and treatment. Plaintiff reasonably believed that Defendant would keep Plaintiff's PII/PHI secure.

Defendant's Collection of Patients' PII/PHI

42. Defendant acknowledges that it obtains, stores and transmits a substantial amount of personal and medical information from its patients. The type of information is detailed in Defendant's Privacy Policy (last updated August 2021),²⁵ which states that Defendant collects the following categories of personal information from patients:

- Personal Data (Any information that directly, indirectly, or in connection with other information — including a personal identification number — allows for the identification or identifiability of a natural person); Usage Data; Tracker; unique device identifiers for advertising (Google Advertiser ID or IDFA, for example); email address; first name; last name; phone number; Data communicated while using the service.

43. For California consumers, Defendant's Privacy Policy identifies the rights of California residents regarding their personal information pursuant to the California Consumer Privacy Act ("CCPA"). These rights include requesting disclosure of the information collected, the purpose for collecting the information, and any third parties with whom the information is sold or disclosed. Additionally, the rights under the CCPA identified by Defendant's Privacy Policy include requesting

²⁵ See Defendant's Privacy Policy, available at <https://lifelongmedical.org/privacy-policy-2/>

1 deletion of the personal information, opting out of have personal information sold to third parties, and
2 receiving information that identifies any third party that has received personal information.

3 44. The CCPA Privacy Policy sets forth the categories of personal information Defendant
4 collects. This includes the following: identifiers (e.g., name, address, unique personal identifier,
5 online identifier, Internet Protocol address, email address, social security number, telephone number,
6 insurance information); and internet usage information (e.g., browsing history, search history, usage
7 data, cookies, and information regarding your interaction with an Internet Web site, application, or
8 advertisement).

9 ***Defendant's Promises to Safeguard Patient PII/PHI***

10 45. Defendant promises that it "takes appropriate security measures to prevent
11 unauthorized access, disclosure, modification, or unauthorized destruction of the Data."²⁶

12 46. Defendant claims it uses "industry standard physical, technical and administrative
13 security measures and safeguards to protect the confidentiality and security of your personal
14 information."²⁷

15 47. Defendant warns that "since the Internet is not a 100 percent secure environment, we
16 cannot guarantee, ensure, or warrant the security of any information you transmit to us. There is no
17 guarantee that information may not be accessed, disclosed, altered, or destroyed by breach of any of
18 our physical, technical, or managerial safeguards. It is your responsibility to protect the security of
19 your login information."

20 48. Defendant's Terms of Use expressly references Defendant's Privacy Policy.

21 ***The Data Breach***

22 49. On August 24, 2021, Defendant sent Plaintiff and other similarly situated patients the
23 Letter with the title, "*IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY*."²⁸ The Letter
24 stated, "We are writing with important information regarding a recent security incident that occurred
25
26

27 ²⁶ https://lifelongmedical.org/privacy-policy-2/#california_info.

28 ²⁷ *Id.*

²⁸ An exemplar of the Letter is attached hereto as **Exhibit A**.



1 at Netgain, a third party vendor that provides services to certain healthcare providers, including
2 LifeLong Medical Care.”

3 50. The Letter went on to state that the ransomware attack occurred November 24, 2020
4 and that on February 25, 2021, Netgain’s investigation determined that certain files were accessed
5 and or acquired including Defendant’s. Further the Letter stated that on or around August 9, 2021,
6 through its investigation Defendant determined that Plaintiff and other similarly situated patients’
7 PII/PHI including their names, social security numbers, dates of birth, patient cardholder numbers,
8 and treatment/diagnosis information had been accessed and/or acquired by unauthorized persons.

9 51. According to Defendant’s Letter, the information in the Data Breach impacted
10 Plaintiff’s PII and/or PHI, including Plaintiff’s name, social security number, date of birth, and patient
11 cardholder number.

12 52. In the Letter, Defendant offered patients a one-year complimentary membership to
13 Equifax’s Credit Watch Gold identity theft program.

14 53. Additionally, in the Letter, Defendant offered a limited number of steps on how to
15 protect against identity theft and fraud. These steps included reviewing financial account statements
16 and credit reports.

17 54. For California residents, the Letter did not identify the rights of consumers under
18 CCPA.

19 55. Based upon the information posted on the U.S. Department of Health and Human
20 Services’ (HHS) official website, on 08/25/2021, Defendant reported to the HHS Office for Civil
21 Rights that the Data Breach described herein as affecting **115,448 persons**.

22 56. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA
23 covered entities to provide notification following a breach of unsecured protected health information.
24 Following a breach of unsecured protected health information, covered entities must provide
25 notification of the breach to affected individuals. Covered entities must *only* provide the required
26 notifications if the breach involved unsecured protected health information. Unsecured protected
27 health information is protected health information that has not been rendered unusable, unreadable,
28 or indecipherable to unauthorized persons through the use of a technology or methodology specified



1 by the Secretary of the U.S. Department of Health and Human Services in guidance. Under approved
 2 guidance of the U.S. Department of Health and Human Services, protected health information (“PHI”)
 3 is rendered unusable, unreadable, or indecipherable to unauthorized individuals if (1) electronic PHI
 4 has been encrypted as specified in the HIPAA Security Rule by “the use of an algorithmic process to
 5 transform data into a form in which there is a low probability of assigning meaning without use of a
 6 confidential process or key” (45 CFR § 164.304 definition of encryption) and (2) such confidential
 7 process or key that might enable decryption has not been breached.

8 57. By reporting the Data Breach discussed herein to the U.S. Department of Health and
 9 Human Services and by sending its Letter providing notice of the Data Breach, Defendant determined
 10 and has effectively affirmed that Plaintiff and the Class’ electronic PII/PHI was either not encrypted
 11 at all, or if it was encrypted, the encryption has been breached by the unauthorized third party. Further,
 12 because Plaintiff and the Class’ identifiable medical information contained in Netgain’s network
 13 server was not rendered unusable, unreadable, or indecipherable, the unauthorized third party or
 14 parties who accessed and/or exfiltrated Plaintiff and the Class’ was able to and did in fact view
 15 Plaintiff and the Class members’ PII/PHI.

16 ***Defendant’s Notice of Data Breach***

17 58. On or around August 24, 2021, Defendant sent Plaintiff and other similarly situated
 18 patients affected by the Data Breach the data breach notification letter referenced above.

19 59. Pursuant to California Civ. Code § 1798.82(a)(1), data breach notification letters must
 20 be sent to residents of California “whose unencrypted personal information was, or is reasonably
 21 believed to have been, acquired by an unauthorized person” due to a “breach of the security of the
 22 system[.]”

23 60. Plaintiff and the Class members’ PII/PHI is “personal information” as defined by
 24 California Civ. Code § 1798.82(h).

25 61. California Civ. Code § 1798.82(g) defines “breach of the security of the system” as
 26 the “unauthorized acquisition of computerized data that compromises the security, confidentiality, or
 27 integrity of personal information maintained by the person or business.”



1 62. The Data Breach was a “breach of the security of the system” as defined by California
2 Civ. Code § 1798.82(g).

3 63. Thus, Defendant filed and disseminated its breach notification Letter because Plaintiff
4 and the Class members’ unencrypted PII/PHI was accessed and viewed by an unauthorized person or
5 persons as a result of the Data Breach.

6 64. Defendant’s Notice of the Data Breach letter sent to Plaintiff and other putative Class
7 members is inadequate and fails to provide sufficient detail. Defendant states only that it “[o]n
8 November 24, 2020, Netgain discovered anomalous network activity. Through Netgain’s
9 investigation, it was later determined that Netgain was the victim of a ransomware attack” and that
10 “[o]n February 25, 2021, Netgain’s investigation determined that certain files were accessed and/or
11 acquired without authorization” and thus Defendant “[t]hereafter . . . conducted a thorough review
12 of the contents of the acquired files to determine if they contained any sensitive information” which
13 Defendant then identified Plaintiff and other putative class members PII and/or PHI had been
14 compromised. It is unclear whether the intrusion, or intrusions, occurred on separate days or every
15 day or who long. It also fails to indicate whether the breach was only of existing patient PII/PHI or
16 whether it also included PII/PHI collected from former and/or potential patients.

17 65. Defendant’s vague description of the Data Breach leaves Plaintiff and Class members
18 at continuing risk. By failing to adequately inform Plaintiff and Class members of the specific details
19 surrounding the breach Plaintiff and Class members are unable to adequately protect themselves
20 against identity theft and other damages.

21 66. Further, Defendant offered Plaintiff and Class members little to assist them with any
22 fall-out from the Data Breach or to advise them of the extent of the potential threat they face as a
23 result of their sensitive PII/PHI being in the hands of criminals. Defendant’s offer of a one-year
24 subscription to Equifax’s Credit Watch Gold identity theft protection program is insufficient where
25 Plaintiff and Class members are now at imminent and continued increased risk of identity theft for
26 years to come as a result of the Data Breach.

67. Defendant also fails to explain why it waited so to notify Plaintiff and Class members about the Data Breach. This delayed Plaintiff's and Class members' ability to take necessary precautions to protect themselves from identity theft and other fraud.

Defendant Knew or Should Have Known PII/PHI Are High Risk Targets

68. Defendant knew or should have known that PII and PHI like the information obtained, maintained and stored on Defendant's servers and network, including its email system, is a high-risk target for identity thieves.

69. The Identity Theft Resource Center reported that the business sector had the largest number of breaches in 2018. According to the ITRC this sector suffered 571 data breaches exposing at least 415,233,143 million records in 2018.²⁹ Further, the ITRC identified "hacking" as the most common form of data breach in 2018, accounting for 39% of data breaches.

70. Companies are increasingly being targeted with phishing attacks. A phishing attack is a method of infiltrating for the purpose of removing data for the purpose of viewing and using it to commit acts such as identity theft and otherwise wrongfully obtaining money or other things of value. Sometimes the person who engaged in phishing uses the data obtained to commit cyber fraud and sometime the person sells the data to other identity thieves. Either way, the information must be viewed to be of any use or to confirm the contents of the data before being sold.

71. Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate person or entity so that the recipient provides sensitive data. The hacker cannot do it by him or herself. A phishing incident requires the email system to allow the phishing email to reach the email recipient, for the email recipient to click on a link, provide login credentials, download a file, or take similar affirmative action to allow the hacker to compromise the email recipient's system. The information is then used to access important accounts such as Plaintiff's and Class members' PII/PHI.

²⁹ Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, available at https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

72. Phishing does not just happen. To be successful, phishing relies on a series of affirmative acts by a company and its employees. This is because computers must be told what to do; they do not make independent decisions. Rather, they rely on instructions and actions from users and programmers. A successful phishing attack also requires an intentional affirmative act on the part of, for example, a company employee, such as clicking a link, downloading a file, or providing sensitive information.

73. Phishing attempts are extremely common. According to the Anti-Phishing Working Group's ("APWG") Phishing Activity Trends Report for Q2 2020, the first half of the year saw 146,994 reported phishing attacks.³⁰ Verizon's 2020 Data Breach Investigation Report found that phishing is one of the top data breach threats, with 22 percent of data breaches involving phishing.

74. Phishing is one-way identity thieves, scammers and fraudsters steal information. Comparitech explains the goal of phishing is to trick victims into divulging confidential or personal information that can then be used for fraudulent purposes, like identity theft.³¹ The HIPAA Journal explains that phishing attacks on the healthcare industry typically have one of two objectives – to obtain access to PHI or to deliver ransomware. PHI is a valuable commodity on the black market because it can be used to create false identities, obtain free medical treatment, and commit insurance fraud. Thus, the goal of phishing is to obtain and use compromised data so that it may be used to commit fraud.³²

75. The APWG describes phishing as a crime employing both social engineering and technical subterfuge to steal personal identity data and account credentials. Social engineering schemes prey on unwary victims by fooling them into believing they are dealing with a trusted, legitimate party, such as by using deceptive email addresses and email messages. Phishing schemes are designed to lead victims to counterfeit websites that trick recipients into divulging personal data such as usernames and passwords. Technical subterfuge schemes plant malware onto computers to

³⁰ https://docs.apwg.org/reports/apwg_trends_report_q2_2020.pdf

³¹ <https://www.comparitech.com/blog/information-security/common-phishing-scams-how-to-avoid/>

³² <https://www.hipaajournal.com/protect-healthcare-data-from-phishing/>



1 steal credentials directly, often using systems that intercept victims' account usernames and
2 passwords or misdirect victims to counterfeit websites.

3 76. The HIPPA Journal describes that most phishing attacks on the healthcare industry are
4 deployed by email. The communications generally look authentic and instruct employees to follow a
5 link to a web page – where they will be asked to complete some action that will trigger a malware
6 download or enter their username and password to continue. In addition to ransomware, the malware
7 may be in the form of surveillance software such as adware and keystroke loggers that can be
8 downloaded to follow an employee's online activities and record their usernames and passwords.
9 Other types of malicious software can be downloaded to create gateways for hackers to enter an
10 organization's network remotely. If the phishing attempt has been successful in obtaining a username
11 and password, the hacker will likely be able to access PHI almost immediately.³³

12 77. Phishing attacks are successful because a company has not employed adequate
13 security procedures such as (1) training employees on how to recognize and report phishing attacks
14 and conducting mock phishing scenarios; (2) deploying spam filters that can be enabled to recognize
15 and prevent emails from suspicious sources from ever reaching the inbox of employees; (3) keeping
16 all systems current with the latest security patches and updates; (4) installing antivirus solutions and
17 monitoring the antivirus status on all equipment; (5) developing a security policy that includes
18 password expiration and complexity and using two factor authentication to prevent hackers who have
19 compromised a user's credentials from ever gaining access; (6) encrypting all sensitive company
20 information; (7) using only well-configured devices and employing good end point defenses that can
21 stop malware from installing, even if a phishing email is clicked; and (8) implementing policies and
22 procedures for responding quickly to incidents.

23 78. Prior to the Data Breach, there were many reports of high-profile data breaches that
24 should have put a company like Defendant on high alert and forced it to closely examine its own
25 security procedures, as well as those of third parties with which it did business and gave access to
26 their subscriber PII/PHI.

27
28
³³ *Id.*



79. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018. Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry. The 525 reported breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.

80. In light of recent high profile data breaches at other healthcare partner and provider companies, including, American Medical Collection Agency (25 million patients, March 2019) University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that Plaintiff and Class members electronic records would be targeted by cybercriminals.

81. As such, Defendant was aware that PII/PHI is at high risk of theft, and consequently should have but did not take appropriate and standard measures to safeguard Plaintiff's and Class members' PII/PHI against cyber-security attacks that Defendant should have anticipated and guarded against, including a ransomware attack.

82. At no point in time did Plaintiff give written authorization for Defendant to reveal or disclose Plaintiff's PII/PHI to any other person, including Netgain. Plaintiff was informed and never specifically consented to Plaintiff's PII, PHI, and/or confidential medical information being disclosed to Netgain.

83. Pursuant to Cal. Civ. Code § 56.10(a), a provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care **without first obtaining an authorization**, except as provided in subdivision (b) or (c).

84. Subdivision (b) of Cal. Civ. Code § 56.10 provides an exhaustive list of circumstances under which Defendant *must* disclose medical information without prior authorization.

85. Subdivision (c) of Cal. Civ. Code § 56.10 provides an exhaustive list of circumstances under which Defendant *may* disclose medical information without prior authorization.

1 86. Neither subdivision (b) or (c) of Cal. Civ. Code § 56.10 include disclosing allowing
2 access to Plaintiffs' and the Class members' medical information to an unauthorized vendor in
3 connection with fundraising activities, or other unidentified unauthorized persons as an exception to
4 the mandatory authorization required under Cal. Civ. Code § 56.10(a).

5 87. Further, Cal. Civ. Code 56.10(d) states that unless "expressly authorized by a patient,
6 enrollee, or subscriber, or as provided by subdivisions (b) and (c), a provider of health care . . . shall
7 not intentionally share, sell, use for marketing, or otherwise use medical information for a purpose
8 not necessary to provide health care services to the patient."

9 88. "Authorization" is defined under the CMIA as obtaining permission in accordance
10 with Cal. Civ. Code § 56.11 (or § 56.21 in the context of an employer disclosing medical information).

11 89. Defendant did not obtain valid authorization from as defined under Cal. Civ. Code §
12 56.11 of the CMIA prior to disclosing Plaintiff's and the Class members' personal data, including
13 PII, PHI and/or medical information to Netgain or other unidentified unauthorized third parties.

14 90. Through the above, Defendant recklessly failed to take adequate precautions to
15 safeguard the confidential medical information of Plaintiff and similarly situated members of the
16 Class.

17 91. Through the above conduct, Defendant carelessly, recklessly, negligently, and
18 impermissibly revealed Plaintiff' and the Class members' sensitive PII/PHI to Netgain; and as a result
19 of disclosing their personal data to Netgain, Defendant allowed and was the cause of Plaintiff's and
20 the Class members' personal data, including PII, PHI, and medical information to be accessed,
21 viewed, and acquired by unauthorized third parties.

22 92. In selecting Defendant as a healthcare provider, Plaintiff relied on Defendant to not
23 disclose their PII, PHI and/or confidential information to unauthorized third parties, including
24 Netgain, and entrusted Defendant to use adequate privacy and security provisions with regard to
25 Plaintiff's PII and PHI.

26 93. Upon information and belief, Netgain has not provided verification or further
27 information to Defendant regarding the disposition of the data to confirm that the stolen data has been
28 recovered or destroyed, nor does Defendant or Netgain know whether the other unidentified

1 unauthorized third parties who accessed and/or exfiltrated the data maintained the data in a manner
 2 to prevent others from accessing or acquiring Plaintiffs' and the Class members PII, PHI and/or
 3 medical information.

4 94. Plaintiff has been distressed by the fact that Defendant so carelessly disclosed
 5 Plaintiff's PII and PHI to unauthorized persons in violation of Cal. Civ. Code §§ 56, et seq. Plaintiff
 6 has suffered from increased stress, embarrassment, humiliation, frustration, fear and anxiety and bears
 7 an imminent and continuing increased risk of identity theft, including medical identity theft, as a
 8 result of Defendant's reckless exposure of Plaintiff's PII and PHI unauthorized persons.

9 **CLASS DEFINITION AND ALLEGATIONS**

10 95. Pursuant to Cal. Code Civ. Proc. § 382 and Cal. Civ. Code § 1781, Plaintiff seeks to
 11 represent and intends to certify the following class:

12 All residents of California whose PII and/or PHI was compromised in the
 13 Data Breach disclosed by Defendant's Letter (the "Class").

14 96. Excluded from the Class are: (1) Defendant and its officers, directors, employees,
 15 principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the agents, affiliates,
 16 legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such persons or entities
 17 described herein; and (3) the Judge(s) assigned to this case and any members of their immediate
 18 families.

19 97. Certification of Plaintiff's claims for classwide treatment is appropriate because
 20 Plaintiff can prove the elements of the claims on a classwide basis using the same evidence as would
 21 be used to prove those elements in individual actions alleging the same claims.

22 98. The Class members are so numerous and geographically dispersed throughout
 23 California that joinder of all Class members would be impracticable. While the exact number of class
 24 members is unknown, Defendant acknowledges the Data Breach, and reports estimate the breach to
 25 include over 200,000 patients, including Plaintiff and Class members. Plaintiff therefore believes that
 26 the Class is so numerous that joinder of all members is impractical.

27 99. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed
 28 members of the Class, had their PII/PHI compromised in the Data Breach. Plaintiff and Class

members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

100. There is a well-defined community of interest in the common questions of law and fact affecting Class members. The questions of law and fact common to Class members predominate over questions affecting only individual Class members, and include without limitation:

- a. Whether Defendants participated in or committed the wrongful conduct alleged herein;
 - b. Whether Defendants' acts, transactions, or course of conduct constitute the violations of law alleged herein;
 - c. Whether Plaintiff and the members of the Class sustained and/or continue to sustain damages attributable to Defendants' conduct, and, if so, the proper measure and appropriate formula to be applied in determining such damages; and
 - d. Whether Plaintiff and the members of the Class are entitled to damages, including injunctive and/or any other equitable relief.
- (a) Whether Plaintiff and each Class member are entitled to damages and other equitable relief.

101. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that Plaintiff has no interests adverse to or that conflict with the Class Plaintiff seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

102. A class action is superior to any other available method for the fair and efficient adjudication of this controversy since individual joinder of all Class members is impractical. Furthermore, the expenses and burden of individual litigation would make it difficult or impossible for the individual members of the Class to redress the wrongs done to them, especially given that the damages or injuries suffered by each individual member of the Class are outweighed by the costs of suit. Even if the Class members could afford individualized litigation, the cost to the court system

1 would be substantial and individual actions would also present the potential for inconsistent or
 2 contradictory judgments. By contrast, a class action presents fewer management difficulties and
 3 provides the benefits of single adjudication and comprehensive supervision by a single court.

4 103. Defendant has acted or refused to act on grounds generally applicable to the entire
 5 Class, thereby making it appropriate for this Court to grant final injunctive, including public
 6 injunctive relief, and declaratory relief with respect to the Class as a whole.

7 **CAUSES OF ACTION**

8 **FIRST CAUSE OF ACTION**

9 **Violation of the California Consumer Privacy Act of 2018 (“CCPA”) (Cal. Civ. Code §§ 1798.100, *et seq.*)**

10 104. Plaintiff re-alleges and incorporates by reference all proceeding paragraphs as if fully
 11 set forth herein.

12 105. As more personal information about consumers is collected by businesses, consumers’
 13 ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses
 14 with their personal information on the understanding that businesses will adequately protect it from
 15 unauthorized access and disclosure. The California Legislature explained: “The unauthorized
 16 disclosure of personal information and the loss of privacy can have devastating effects for individuals,
 17 ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to
 18 destruction of property, harassment, reputational damage, emotional stress, and even potential
 19 physical harm.”³⁴

20 106. As a result, in 2018, the California Legislature passed the CCPA, giving consumers
 21 broad protections and rights intended to safeguard their personal information. Among other things,
 22 the CCPA imposes an affirmative duty on businesses that maintain personal information about
 23 California residents to implement and maintain reasonable security procedures and practices that are
 24 appropriate to the nature of the information collected. Defendant failed to implement such procedures
 25 which resulted in the Data Breach.

26
 27
 28 ³⁴ California Consumer Privacy Act (CCPA) Compliance, <https://buyergenomics.com/ccpa-compliance/>.



1 107. It also requires “[a] business that discloses personal information about a California
2 resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third
3 party implement and maintain reasonable security procedures and practices appropriate to the nature
4 of the information, to protect the personal information from unauthorized access, destruction, use,
5 modification, or disclosure.” Cal. Civ. Code § 1798.81.5(c).

6 108. Section 1798.150(a)(1) of the CCPA provides: “Any consumer whose nonencrypted
7 or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access
8 and exfiltration, theft, or disclosure as a result of the business’ violation of the duty to implement and
9 maintain reasonable security procedures and practices appropriate to the nature of the information to
10 protect the personal information may institute a civil action for” statutory or actual damages,
11 injunctive or declaratory relief, and any other relief the court deems proper.

12 109. Plaintiff and the Class members are “consumer[s]” as defined by Civ. Code
13 § 1798.140(g) because they are “natural person[s] who [are] California resident[s], as defined in
14 Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1,
15 2017.”

16 110. Defendant is a “business” as defined by Civ. Code § 1798.140(c) because Defendant:

17 a. is a “sole proprietorship, partnership, limited liability company,
18 corporation, association, or other legal entity that is organized or operated for the
19 profit or financial benefit of its shareholders or other owners”;

20 b. “collects consumers’ personal information, or on the behalf of
21 which is collected and that alone, or jointly with others, determines the purposes
22 and means of the processing of consumers’ personal information”;

23 c. does business in California; and

24 d. has annual gross revenues in excess of \$25 million; or annually
25 buys, receives for the business’ commercial purposes, sells or shares for
26 commercial purposes, alone or in combination, the personal information of 50,000
27 or more consumers, households, or devices; or derives 50 percent or more of its
28 annual revenues from selling consumers’ personal information.



111. The PII/PHI taken in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff's and the Class members' unencrypted first and last names and Social Security number, among other information.

112. Plaintiff's and the putative Class' PII/PHI was subject to unauthorized access, exfiltration, theft, and/or disclosure because their PII/PHI, including name, social security number, date of birth, patient cardholder number, treatment/diagnosis information, was wrongfully accessed, viewed and/or acquired by unauthorized third parties.

113. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff's and the Class members' PII. Defendant failed to implement reasonable security procedures to prevent an attack on its server or network, including its email system, by hackers and to prevent unauthorized access of Plaintiff's and the Class members' PII as a result of this attack.

114. On September 17, 2021, Plaintiff provided Defendant with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). *See Exhibit B* attached hereto. In the event Defendant does not cure the violation within 30 days, Plaintiff intends to amend this complaint to pursue statutory damages as permitted by Civil Code § 1798.150(a)(1)(A).

115. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff seeks actual and statutory damages, injunctive relief, including public injunctive relief, declaratory relief, and any other relief as deemed appropriate by the Court.

SECOND CAUSE OF ACTION
Violation of the California Confidentiality of Medical Information Act ("CMIA")
(Cal. Civ. Code §§ 56, *et seq.*)

116. Plaintiff re-alleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

117. Section 56.10(a) of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization[.]"



118. Defendant is a “contractor” within the meaning of Civil Code § 56.05(d) and/or a “provider of healthcare” within the meaning of Civil Code § 56.06 and/or a “business organized for the purpose of maintaining medical information” and/or a “business that offers software or hardware to consumers . . . that is designed to maintain medical information” within the meaning of Civil Code § 56.06(a) and (b), and maintained and continues to maintain “medical information,” within the meaning of Civil Code § 56.05(j), for “patients” of Defendant, within the meaning of Civil Code § 56.05(k).

119. Plaintiff and all members of the Class are “patients” within the meaning of Civil Code § 56.05(k) and are “endanger[ed]” within the meaning of Civil Code § 56.05(e) because Plaintiff and the Class fear that disclosure of their medical information could subject them to harassment or abuse.

120. Plaintiff and the respective Class members, as patients, had their PHI, or individually identifiable “medical information,” within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored by Defendant.

121. At all relevant times, Defendant had a legal duty to protect the confidentiality of Plaintiff’s personal information and medical information.

122. In violation of Civil Code § 56.10(a), Defendant disclosed Plaintiff’s and the Class members’ medical information without first obtaining an authorization. Plaintiff’s and the Class members’ medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant’s violation of Civil Code § 56.10(a).

123. In violation of Civil Code § 56.10(e), Defendant further disclosed Plaintiff’s and the Class members’ medical information to persons or entities not engaged in providing direct health care services to Plaintiff or the Class members or their providers of health care or health care service plans or insurers or self-insured employers.

124. Defendant violated Civil Code § 56.101 of the CMIA through its failure to maintain and preserve the confidentiality of the medical information of Plaintiff and the Class.

125. In violation of Civil Code § 56.101(a), Defendant created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiff’s and the Class members’ medical information in a manner that failed to preserve and breached the confidentiality of the information contained



1 therein. Plaintiff's and the Class members' medical information was viewed by unauthorized
2 individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(a).

3 126. In violation of Civil Code § 56.101(a), Defendant negligently created, maintained,
4 preserved, stored, abandoned, destroyed, or disposed of Plaintiff's and the Class members' medical
5 information. Plaintiff's and the Class members' medical information was viewed by unauthorized
6 individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(a).

7 127. Plaintiff's and the Class members' medical information that was the subject of the
8 Data Breach included "electronic medical records" or "electronic health records" as referenced by
9 Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

10 128. Plaintiff's and the Class members' medical information was viewed by unauthorized
11 individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(b)(1)(A).

12 129. Defendant violated Civil Code § 56.36 of the CMIA through its failure to maintain
13 and preserve the confidentiality of the medical information of Plaintiff and the Class.

14 130. As a result of Defendant's above-described conduct, Plaintiff and the Class have
15 suffered damages from the unauthorized disclosure and release of their individual identifiable
16 "medical information" made unlawful by Civil Code §§ 56.10, 56.101, 56.36.

17 131. As a direct and proximate result of Defendant's above-described wrongful actions,
18 inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach,
19 and violation of the CMIA, Plaintiff and the Class members have suffered (and will continue to suffer)
20 economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent,
21 immediate and the continuing increased risk of identity theft, identity fraud and medical fraud – risks
22 justifying expenditures for protective and remedial services for which they are entitled to
23 compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI,
24 (iv) statutory damages under the California CMIA, (v) deprivation of the value of their PII/PHI, for
25 which there is a well-established national and international market, and/or (vi) the financial and
26 temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their
27 damages.



132. Plaintiff, individually and for each member of the Class, seeks nominal damages of one thousand dollars (\$1,000) for each violation under Civil Code § 56.36(b)(1), and actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2), injunctive relief, as well as punitive damages of up to \$3,000 per Plaintiff and each Class member, and attorneys' fees, litigation expenses and court costs, pursuant to Civil Code § 56.35.

133. Plaintiff also seeks injunctive relief through an order requiring Defendant to cease its violations of the Civil Code §§ 56, et seq. Among other things, Defendant should be required to cease negligently handling its patients' medical information.

THIRD CAUSE OF ACTION
Violation of the California Unfair Competition Law ("UCL")
(Cal. Bus. & Prof. Code §§ 17200, et seq.)

134. Plaintiff re-alleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

135. The UCL prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the UCL.

136. In the course of conducting its business, Defendant committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class members' PII/PHI, and by violating the statutory and common law alleged herein, including, *inter alia*, California's Confidentiality of Medical Information Act (Civ. Code §§ 56.10(a), (e); 56.101(a), 56.101(b)(1)(A); 56.36), California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.150(a)(1)), the Health Insurance Portability and Accountability Act of 1996, (42 U.S.C. § 1302d; 45 C.F.R. §§ 164.306(a), (d), (e); 164.308(a); 164.312(a), (d), (e); 164.316(a), (b)), Civil Code § 1798.81.5, and Article I, Section 1 of the California Constitution (California's constitutional right to privacy). Plaintiff and Class members reserve the right to allege other violations of law by



1 Defendant constituting other unlawful business acts or practices. Defendant's above-described
2 wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this
3 date.

4 137. Defendant also violated the UCL's unlawful prong by breaching contractual
5 obligations created by its Privacy Policy and by knowingly and willfully or, in the alternative,
6 negligently and materially violating Cal. Bus. & Prof. Code § 22576, which prohibits a commercial
7 website operator from "knowingly and willfully" or "negligently and materially" failing to comply
8 with the provisions of their posted privacy policy. Plaintiff and Class members suffered injury in fact
9 and lost money or property as a result of Defendant's violations of its Privacy Policy.

10 138. Defendant also violated the UCL by failing to adequately and timely notify Plaintiff
11 and Class members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and
12 disclosure of their PII. If Plaintiff and Class members had been adequately and timely notified in an
13 appropriate fashion, they could have taken precautions to safeguard and protect their PII/PHI and
14 identities.

15 139. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary
16 care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and
17 practices in violation of the UCL in that Defendant's wrongful conduct is substantially injurious to
18 consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and
19 unscrupulous. Defendant's practices are also contrary to legislatively declared and public policies that
20 seek to protect PII/PHI and ensure that entities who solicit or are entrusted with personal data utilize
21 appropriate security measures, as reflected by laws such as the CCPA, Article I, Section 1 of the
22 California Constitution, and the FTC Act (15 U.S.C. § 45). The gravity of Defendant's wrongful
23 conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available
24 alternatives to further Defendant's legitimate business interests other than engaging in the above-
25 described wrongful conduct.

26 140. Plaintiff and Class members suffered injury in fact and lost money or property as a
27 result of Defendant's violations of its Privacy Policy and statutory and common law in that a portion
28 of the money Plaintiff and Class members paid for Defendant's products and services went to fulfill



1 the contractual obligations set forth in its Privacy Policy, including maintaining the security of their
 2 PII/PHI, and Defendant's legal obligations and Defendant failed to fulfill those obligations.

3 141. The UCL also prohibits any "fraudulent business act or practice." Defendant's above-
 4 described claims, nondisclosures and misleading statements were false, misleading and likely to
 5 deceive the consuming public in violation of the UCL.

6 142. As a direct and proximate result of Defendant's above-described wrongful actions,
 7 inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach
 8 and their violations of the UCL, Plaintiff and Class members have suffered injury in fact and lost
 9 money or property as a result of Defendant's unfair and deceptive conduct. Such injury includes
 10 paying for a certain level of security for their PII/PHI but receiving a lower level, paying more for
 11 Defendant's products and services than they otherwise would have had they known Defendant was
 12 not providing the reasonable security represented in its Privacy Policy and as in conformance with its
 13 legal obligations. Defendant's security practices have economic value in that reasonable security
 14 practices reduce the risk of theft of patient's PII/PHI.

15 143. Plaintiff and Class members have also suffered (and will continue to suffer) economic
 16 damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and
 17 the continuing increased risk of identity theft and identity fraud – risks justifying expenditures for
 18 protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy,
 19 (iii) breach of the confidentiality of their PII/PHI, (iv) statutory damages under the CCPA,
 20 (v) deprivation of the value of their PII/PHI for which there is a well-established national and
 21 international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring
 22 financial accounts, and mitigating damages.

23 144. Unless restrained and enjoined, Defendant will continue to engage in the above-
 24 described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of
 25 themselves, Class members, and the general public, also seek restitution and an injunction, including
 26 public injunctive relief prohibiting Defendant from continuing such wrongful conduct, and requiring
 27 Defendant to modify its corporate culture and design, adopt, implement, control, direct, oversee,
 28 manage, monitor and audit appropriate data security processes, controls, policies, procedures

1 protocols, and software and hardware systems to safeguard and protect the PII/PHI entrusted to it, as
 2 well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

3 **FOURTH CAUSE OF ACTION**

4 **Breach of Contract**

5 145. Plaintiff re-alleges and incorporates by reference all proceeding paragraphs as if fully
 6 set forth herein.

7 146. Plaintiff and Class members entered into express contracts with Defendant as set forth
 8 in its Terms of Use and Privacy Policy that included Defendant's promise to protect nonpublic
 9 personal information given to Defendant or that Defendant gathered on its own, from disclosure, as
 10 set forth in Defendant's Privacy Policy, which was posted on its website.

11 147. Plaintiff and Class members performed their obligations under the contracts when they
 12 provided their PII/PHI to Defendant in relation to their purchase of insurance products or services
 13 from Defendant.

14 148. By allowing unauthorized users to gain access to Plaintiff's and Class members'
 15 PII/PHI through the Data Breach, Defendant breached these contractual obligations. As a result,
 16 Defendant failed to comply with its own policies, including its Privacy Policy, and applicable laws,
 17 regulations and industry standards for data security and protecting the confidentiality of PII/PHI.
 18 Defendant's breach of contract also violated California Business and Professions Code § 22576,
 19 which prohibits a commercial website operator from "knowingly and willfully" or "negligently and
 20 materially" failing to comply with the provisions of their posted privacy policy.

21 149. By failing to fulfill its contractual obligations under its Terms of Use and Privacy
 22 Policy, Defendant failed to confer on Plaintiff and Class members the benefit of the bargain, causing
 23 them economic injury.

24 150. As a direct and proximate result of the Data Breach, Plaintiff and Class members have
 25 been harmed and have suffered, and will continue to suffer, damages and injuries.

26 //

27 //

28 //

FIFTH CAUSE OF ACTION

Negligence

151. Plaintiff re-alleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

152. Defendant owed various duties to Plaintiff and the Class, including pursuant to the CMIA, as alleged in detail above. Specifically, Defendant owed a duty to Plaintiff and the Class with regard to its manner of collection and maintenance of Plaintiff and the Class members' personal data, including PHI, PII, and medical information.

153. Defendant breached Defendant's respective duties by engaging in the conduct and omissions alleged above and in violation of the CMIA.

154. Defendants are both the actual and legal cause of Plaintiff and the Class' damages.

155. Plaintiff believes and thereon alleges that as a proximate result of Defendant's negligence, Plaintiff and the Class have suffered actual damages and significant emotional distress as described herein and above.

156. Due to the egregious violations alleged herein, Plaintiff asserts that Defendant breached Defendant's respective duties in an oppressive, malicious, despicable, gross and wantonly negligent manner. Defendant's conscious disregard for Plaintiff's privacy rights entitles Plaintiff and the Class to recover punitive damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves individually and all members of the Class, respectfully request that (i) this action be certified as a class action, (ii) Plaintiff be designated representative of the certified class(es), and (iii) Plaintiff's undersigned counsel be appointed as Class Counsel. Plaintiff, on behalf of themself and members of the Class, further requests that upon final trial or hearing, judgment be awarded against Defendant for:

- (i) actual and punitive damages to be determined by the trier of fact;
- (ii) statutory damages;
- (iii) equitable relief, including restitution;
- (iv) appropriate injunctive relief;

- 1 (v) punitive damages;
- 2 (vi) attorneys' fees and litigation expenses under Code of Civil Procedure § 1021.5
- 3 and other applicable law;
- 4 (vii) pre- and post-judgment interest at the highest legal rates applicable; and
- 5 (viii) any such other and further relief the Court deems just and proper.

6 **DEMAND FOR JURY TRIAL**

7 Plaintiff, on behalf of themselves individually and the putative Class, hereby demands a jury trial

8 on all issues so triable.

9

10 Dated: September 17 2021

Respectfully submitted,

11 **KAZEROUNI LAW GROUP, APC**

12

13 By: 

14 Abbas Kazerounian, Esq.
15 Mona Amini, Esq.
16 245 Fischer Avenue, Unit D1
17 Costa Mesa, California 92626
18 Telephone: (800) 400-6808
19 Facsimile: (800) 520-5523
20 ak@kazlg.com
21 mona@kazlg.com

22 *Attorneys for Plaintiff and the Proposed Class*

23

24

25

26

27

28

EXHIBIT A



Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

***IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY***

Dear [REDACTED]

We are writing with important information regarding a recent security incident that occurred at Netgain, a third-party vendor that provides services to certain healthcare providers, including LifeLong Medical Care. We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On November 24, 2020, Netgain discovered anomalous network activity. Through Netgain's investigation, it was later determined that Netgain was the victim of a ransomware attack. On February 25, 2021, Netgain's investigation determined that certain files were accessed and/or acquired without authorization. Thereafter, LifeLong Medical Care conducted a thorough review of the contents of the acquired files to determine if they contained any sensitive information.

What Information Was Involved.

Based on LifeLong Medical Care's comprehensive investigation and document review, we discovered on August 9, 2021 that your full name and the following information were accessed and/or acquired from Netgain's network in connection with this incident: [REDACTED]

What You Can Do.

To date, we are not aware of any reports of identity fraud or improper use of your information as a direct result of this incident. Out of an abundance of caution, we wanted to make you aware of the incident, explain the services we are making available to help safeguard you against identity fraud, and suggest steps that you should take as well. To protect you from potential misuse of your information, we are offering a complimentary one-year membership in Equifax® Credit Watch™ Gold. Equifax® Credit Watch™ Gold is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and Equifax® Credit Watch™ Gold, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. We have also offered suggestions for protecting your medical information.

What We Are Doing.

Data privacy and security are among LifeLong Medical Care's highest priorities. As part of LifeLong Medical Care's ongoing commitment to the security of information, we are working with our third-party vendors to enhance security and oversight.

For More Information.

Please accept our apologies that this incident occurred.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 6:00 a.m. to 6:00 p.m. Pacific Time, except holidays.

Sincerely,

LifeLong Medical Care

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Activation Code: [REDACTED]
 Activation Deadline: [REDACTED]

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁴

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of [REDACTED] then click “Submit” and follow these 4 steps:

1. Register:

Complete the form with your contact information and click “Continue”.

If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. Create Account:

Enter your email address, create a password, and accept the terms of use.

3. Verify Identity:

To enroll in your product, we will ask you to complete our identity verification process.

4. Checkout:

Upon successful verification of your identity, you will see the Checkout Page.

Click ‘Sign Me Up’ to finish enrolling.

You’re done!

The confirmation page shows your completed enrollment.

Click “View My Product” to access the product features.

¹ WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers’ personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers’ personal information is at risk of being traded.

² The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

³ Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer’s identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com

⁴ The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

To sign up for US Mail delivery, dial 1-855-833-9162 for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.

1. **Activation Code:** You will be asked to enter your enrollment code as provided at the top of this letter.
2. **Customer Information:** You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.
3. **Permissible Purpose:** You will be asked to provide Equifax with your permission to access your Equifax credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment.
4. **Order Confirmation:** Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.

2. **Placing a Fraud Alert on Your Credit File.**

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

3. **Consider Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
<https://www.freeze.equifax.com>
1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
<http://www.transunion.com/securityfreeze>
1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. **Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. **Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

6. Protecting Your Medical Information.

We have no evidence that any medical information involved in this incident was or will be used for any unintended purposes. However, the following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with the insurance company or the care provider for any items you do not recognize.

EXHIBIT B



245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523
www.kazlg.com

September 17, 2021

VIA CERTIFIED MAIL

Lifelong Medical Care
c/o Patricia D. Espinosa, Agent for Service
2344 6th Street
Berkeley, CA 94710

Re: Noem Margolies v. Lifelong Medical Care

To Whom It May Concern:

We represent Plaintiff Noem Margolies ("Plaintiff") and all other similarly situated consumers in a putative class action against Lifelong Medical Care ("Defendant") arising out of, *inter alia*, Defendant's failure to provide reasonable security for Plaintiff's and the proposed class members' personal information, which resulted in the unauthorized access, theft, or disclosure of this information (the "Data Breach"). To our knowledge the Data Breach occurred on or around November 24, 2020.

The full claims, including the facts and circumstances surrounding these claims are detailed in Plaintiff's Class Action Complaint, a copy of which is attached and incorporated by reference. Defendant's conduct constitutes violations of California Civil Code §§ 1798.81.5(a)(1) and 1798.150(a)(1) among other consumer protection statutes.

While this letter and the attached Complaint constitute sufficient notice of the claims asserted against Defendant, pursuant to California Civil Code 1798.150(b)(1), Plaintiff demands that, in the event a cure is possible, Defendant is hereby provided the opportunity to actually cure the noticed violations and provide Plaintiff with an express written statement within 30 days that the violations have been cured and that no further violations shall occur. A cure, if possible, requires that all the information taken has been recovered and that Plaintiff and the proposed class members of similarly situated persons are not at any risk of any of the information being used.

Thank you for your time and attention to this matter.

Sincerely,

s/Abbas Kazerounian

Abbas Kazerounian, Esq.
KAZEROUNI LAW GROUP, APC
Direct Line: (800) 400-6808, Ext. 2
E-mail: ak@kazlg.com

[Enclosure]

EXHIBIT "2"

POS-015

ATTORNEY OR PARTY WITHOUT ATTORNEY: STATE BAR NO: NAME: Abbas Kazerounian, Esq. (249203); Mona Amini, Esq. (296829) FIRM NAME: Kazerouni Law Group, APC STREET ADDRESS: 245 Fischer Ave, Unit D1 CITY: Costa Mesa STATE: CA ZIP CODE: 92626 TELEPHONE NO.: (800) 400-6808 FAX NO.: (800) 520-5523 E-MAIL ADDRESS: ak@kazlg.com, mona@kazlg.com ATTORNEY FOR (Name): Plaintiff, Noem Margolies	FOR COURT USE ONLY
SUPERIOR COURT OF CALIFORNIA, COUNTY OF ALAMEDA STREET ADDRESS: 1225 Fallon Street MAILING ADDRESS: CITY AND ZIP CODE: Oakland, CA 94612 BRANCH NAME:	
Plaintiff/Petitioner: Noem Margolies Defendant/Respondent: Lifelong Medical Care	
NOTICE AND ACKNOWLEDGMENT OF RECEIPT—CIVIL	
CASE NUMBER: RG21113030	

TO (insert name of party being served): Lifelong Medical Care

NOTICE

The summons and other documents identified below are being served pursuant to section 415.30 of the California Code of Civil Procedure. Your failure to complete this form and return it within 20 days from the date of mailing shown below may subject you (or the party on whose behalf you are being served) to liability for the payment of any expenses incurred in serving a summons on you in any other manner permitted by law.

If you are being served on behalf of a corporation, an unincorporated association (including a partnership), or other entity, this form must be signed by you in the name of such entity or by a person authorized to receive service of process on behalf of such entity. In all other cases, this form must be signed by you personally or by a person authorized by you to acknowledge receipt of summons. If you return this form to the sender, service of a summons is deemed complete on the day you sign the acknowledgment of receipt below.

Date of mailing: November 12, 2021

Mona Amini, Esq.

(TYPE OR PRINT NAME)

(SIGNATURE OF SENDER—MUST NOT BE A PARTY IN THIS CASE)

ACKNOWLEDGMENT OF RECEIPTThis acknowledges receipt of **(to be completed by sender before mailing)**:

- ☒ A copy of the summons and of the complaint.
- ☐ Other (specify):

(To be completed by recipient):

Date this form is signed: Nov. 15, 2021

Nathan Guest for Lifelong Medical Care

(TYPE OR PRINT YOUR NAME AND NAME OF ENTITY, IF ANY, ON WHOSE BEHALF THIS FORM IS SIGNED)

(SIGNATURE OF PERSON ACKNOWLEDGING RECEIPT, WITH TITLE IF ACKNOWLEDGMENT IS MADE ON BEHALF OF ANOTHER PERSON OR ENTITY)

Page 1 of 1

NOTICE AND ACKNOWLEDGMENT OF RECEIPT — CIVIL

EXHIBIT "3"

SUMMONS
Cross-Complaint
(CITACION JUDICIAL-CONTRADEMANDA)

NOTICE TO CROSS-DEFENDANT:
(AVISO AL CONTRA-DEMANDADO):

NETGAIN TECHNOLOGY, INC., a Minnesota corporation; and ROES 1-50, inclusive

YOU ARE BEING SUED BY CROSS-COMPLAINANT:
(LO ESTÁ DEMANDANDO EL CONTRADEMANDANTE):
 LIFELONG MEDICAL CARE a California corporation

FOR COURT USE ONLY
 (SOLO PARA USO DE LA CORTE)

ELECTRONICALLY FILED
 Superior Court of California
 County of Alameda
 11/29/2021

Chad Finke, Executive Officer / Clerk of the Court

By: Andrel Gospel Deputy

You have 30 CALENDAR DAYS after this summons and legal papers are served on you to file a written response at this court and have a copy served on the cross-complainant. A letter or phone call will not protect you. Your written response must be in proper legal form if you want the court to hear your case. There may be a court form that you can use for your response. You can find these court forms and more information at the California Courts Online Self-Help Center (www.courtinfo.ca.gov/selfhelp), your county law library, or the courthouse nearest you. If you cannot pay the filing fee, ask the court clerk for a fee waiver form. If you do not file your response on time, you may lose the case by default, and your wages, money, and property may be taken without further warning from the court.

There are other legal requirements. You may want to call an attorney right away. If you do not know an attorney, you may want to call an attorney referral service. If you cannot afford an attorney, you may be eligible for free legal services from a nonprofit legal services program. You can locate these nonprofit groups at the California Legal Services Web site (www.lawhelpcalifornia.org), the California Courts Online Self-Help Center (www.courtinfo.ca.gov/selfhelp), or by contacting your local court or county bar association. NOTE: The court has a statutory lien for waived fees and costs on any settlement or arbitration award of \$10,000 or more in a civil case. The court's lien must be paid before the court will dismiss the case.

Tiene 30 DÍAS DE CALENDARIO después de que le entreguen esta citación y papeles legales para presentar una respuesta por escrito en esta corte y hacer que se entregue una copia al contrademandante. Una carta o una llamada telefónica no lo protegen. Su respuesta por escrito tiene que estar en formato legal correcto si desea que procesen su caso en la corte. Es posible que haya un formulario que usted pueda usar para su respuesta. Puede encontrar estos formularios de la corte y más información en el Centro de Ayuda de las Cortes de California (www.sucorte.ca.gov), en la biblioteca de leyes de su condado o en la corte que le quede más cerca. Si no puede pagar la cuota de presentación, pida al secretario de la corte que le dé un formulario de exención de pago de cuotas. Si no presenta su respuesta a tiempo, puede perder el caso por incumplimiento y la corte le podrá quitar su sueldo, dinero y bienes sin más advertencia.

Hay otros requisitos legales. Es recomendable que llame a un abogado inmediatamente. Si no conoce a un abogado, puede llamar a un servicio de remisión a abogados. Si no puede pagar a un abogado, es posible que cumpla con los requisitos para obtener servicios legales gratuitos de un programa de servicios legales sin fines de lucro. Puede encontrar estos grupos sin fines de lucro en el sitio web de California Legal Services (www.lawhelpcalifornia.org), en el Centro de Ayuda de las Cortes de California (www.sucorte.ca.gov), o uniéndose en contacto con la corte o el colegio de abogados locales. AVISO: Por ley, la corte tiene derecho a reclamar las cuotas y los costos exentos por imponer un gravamen sobre cualquier recuperación de \$10,000 ó más de valor recibida mediante un acuerdo o una concesión de arbitraje en un caso de derecho civil. Tiene que pagar el gravamen de la corte antes de que la corte pueda desechar el caso.

The name and address of the court is:
 (El nombre y dirección de la corte es):

Alameda Superior Court
 1221 Oak Street
 Oakland, CA 94612

SHORT NAME OF CASE (from Complaint): (Nombre de Caso):

Margolies v. Lifelong Medical Care

CASE NUMBER: (Número del Caso):

RG21113030

The name, address, and telephone number of cross-complainant's attorney, or cross-complainant without an attorney, is:

(El nombre, la dirección y el número de teléfono del abogado del contrademandante, o del contrademandante que no tiene abogado, es): Nathan A. Guest Tel: (310) 481-7600 / Fax (310) 481-7650

WOOD, SMITH, HENNING & BERMAN LLP

Chad Finke, Executive Officer / Clerk of the Court

10960 Wilshire Boulevard, 18th Floor, Los Angeles, California 90024-3804

DATE:

(Fecha) 11/29/2021

Clerk, by

(Secretario)

Andrel Gospel

, Deputy

(Adjunto)

(For proof of service of this summons, use Proof of Service of Summons (form POS-010).)

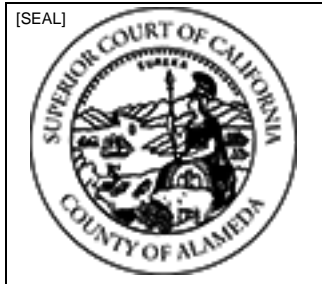
(Para prueba de entrega de esta citación use el formulario Proof of Service of Summons (POS-010).)

NOTICE TO THE PERSON SERVED: You are served

1. ☐ as an individual cross-defendant.
2. ☐ as the person sued under the fictitious name of (specify):
3. ☐ on behalf of (specify):

under: <input type="checkbox"/> CCP 416.10 (corporation)	<input type="checkbox"/> CCP 416.60 (minor)
<input type="checkbox"/> CCP 416.20 (defunct corporation)	<input type="checkbox"/> CCP 416.70 (conservatee)
<input type="checkbox"/> CCP 416.40 (association or partnership)	<input type="checkbox"/> CCP 416.90 (authorized person)
<input type="checkbox"/> other (specify):	
4. ☐ by personal delivery on (date):

[SEAL]



ELECTRONICALLY FILED

Superior Court of California,
County of Alameda
11/29/2021 at 05:14:09 PM

By: Andrei Gospel, Deputy Clerk

Nathan A. Guest (State Bar No. 330167)
nguest@wshblaw.com
WOOD, SMITH, HENNING & BERMAN LLP
10960 Wilshire Boulevard, 18th Floor
Los Angeles, California 90024-3804
Phone: 310-481-7600 ♦ Fax: 310-481-7650

Attorneys for Defendant/Cross-Complainant, LIFELONG MEDICAL CARE, a
California corporation

**SUPERIOR COURT OF THE STATE OF CALIFORNIA
FOR THE COUNTY OF ALAMEDA – COMPLEX CIVIL**

NOEM MARGOLIES, individually and on
behalf of all others similarly situated,

Plaintiffs,

v.

LIFELONG MEDICAL CARE, a California
corporation; and DOES 1-50, inclusive,

Defendant(s).

Lead Case No. RG21113030

CROSS-COMPLAINT FOR:

- 1. EQUITABLE/IMPLIED INDEMNITY;**
- 2. IMPLIED CONTRACTUAL INDEMNITY;**
- 3. BREACH OF WRITTEN CONTRACT;**
- 4. CONTRIBUTION;**
- 5. APPORTIONMENT OF FAULT; and**
- 6. DECLARATORY RELIEF.**

LIFELONG MEDICAL CARE a California
corporation,

Cross-Complainant,

v.

NETGAIN TECHNOLOGY, INC., a
Minnesota corporation; and ROES 1-50,
inclusive,

Cross-Defendants.

[Assigned for All Purposes to Judge Evelio Grillo]

Action Filed: 09/17/21

Trial Date: None Set

AND ALL RELATED CROSS-ACTIONS.

Cross-Complainant, LIFELONG MEDICAL CARE (hereinafter "Cross-Complainant")
files this Cross-Complaint for causes of action against Cross-Defendants, and each of them, as

1 follows:

2 **GENERAL ALLEGATIONS**

3 1. This Cross-Complaint arises from the Complaint filed by Plaintiffs NOEM
4 MARGOLIES, individually and on behalf of all others similarly situated (hereinafter "Plaintiffs")
5 which arose as a result of Cross-Defendant NETGAIN TECHNOLOGY, INC.'s (hereinafter
6 "NETGAIN") failure to take all reasonable steps to ensure that the non-public confidential
7 information of Plaintiffs was not subject to unauthorized access and/or disclosure, pursuant to
8 Section XI of the agreement with Cross-Complainant.

9 2. At all times herein mentioned, Cross-Complainant is a non-profit healthcare
10 provider that serves patients in the State of California, with its principal place of business at 2344
11 Sixth Street, Berkeley, California 94710.

12 3. At all times herein mentioned, Cross-Complainant is informed and believes, and
13 based thereon alleges that at all times herein mentioned, that Cross-Defendant is a Minnesota
14 corporation, with its principal place of business at 720 West St. Germain Street, St. Cloud,
15 Minnesota, 56301, doing business in the State of California, at all times relevant to the subject
16 matter of this action.

17 4. Cross-Complainant is informed and believes, and based thereon alleges that at all
18 times herein mentioned, Cross-Defendant, NETGAIN, is a cloud hosting and information
19 technology service provider for healthcare organizations, including Cross-Complainant.

20 5. Cross-Complainant is presently unaware of the true names and capacities and
21 liability of Cross-Defendants named herein as ROES 1 - 50, inclusive, and Cross-Complainant
22 will seek leave of court to amend this Cross-Complaint to allege their true names and capacities
23 after they have been ascertained.

24 6. Cross-Complainant is informed and believes and based thereon alleges that each of
25 the Cross-Defendants, including ROES 1 - 50, inclusive, are in some manner legally responsible
26 for the acts and omissions alleged herein, and actually and proximately caused and contributed to
27 the various injuries and damages referred to herein.

28 ///

WOOD, SMITH, HENNING & BERMAN LLP
 Attorneys at Law
 10960 WILSHIRE BOULEVARD, 18TH FLOOR
 LOS ANGELES, CALIFORNIA 90024-3804
 TELEPHONE 310-481-7600 ♦ FAX 310-481-7650

7. Cross-Complainant is informed and believes and based thereon alleges, that at all times herein mentioned, Cross-Defendants, including ROES 1 through 50, and each of them, was the agent, partner, co-developer, joint venturer, lender, predecessor in interest, successor in interest, and/or employee of each of the remaining Cross-Defendants, including ROES 1 through 50, and each of them, and were at all times herein mentioned acting within the course and scope of such agency and/or employment.

8. At all times herein mentioned, a written contract¹ existed between Cross-Complainant and Cross-Defendant NETGAIN, the terms of which shall be according to proof at time of trial. On or about December 21, 2015, Cross-Complainant entered into a written contract ("Agreement") with Cross-Defendant NETGAIN. The Agreement sets forth terms and conditions under which Cross-Defendant NETGAIN, agrees to provide Cross-Complainant computer related services. Pursuant to the Agreement, Cross-Defendant NETGAIN, acknowledges that it has access to non-public/confidential information of the Plaintiffs (Cross-Complaint's patients). The Agreement prohibits Netgain from disclosing this information to any person outside of its company. Netgain agreed to take all reasonable steps to ensure fulfillment of this obligation.

9. Cross-Complainant is informed and believes thereon alleges that at all times herein mentioned, that on November 24, 2020, Cross-Defendant NETGAIN, sustained a ransomware attack (the "Netgain Incident"). As a result of the ransomware attack on NETGAIN, the personal identifiable information ("PII") and personal health information ("PHI") of approximately 115,000 LIFELONG patients may have been subject to unauthorized access.

10. On or about September 17, 2021, Plaintiffs filed a lawsuit against Cross-Complainant for damages arising out of the Netgain Incident, in the Alameda County Superior Court, Case No. RO21113030, ("Complaint"). Plaintiffs alleged causes of action for (1) violations

¹ A copy of the referenced Agreement is not annexed to the Complaint due to the confidentiality provision in the Agreement. However, a copy of the Agreement can be produced upon consent of all parties or upon Order of the Court.

1 of the California Consumer Privacy Act (CCPA); (2) violations of the Confidentiality of Medical
 2 Information Act (CMIA); (3) violations of the California Unfair Competition Law (UCL); (4)
 3 breach of contract; and (5) negligence.

4 11. Upon information and belief, pursuant to language contained in the Agreement and
 5 as may otherwise apply by law, Cross-Defendant NETGAIN, has an obligation to Cross-
 6 Complainant for all losses or damages arising out of or in connection with the Netgain Incident
 7 that is the subject of Plaintiffs' Complaint.

8
 9 **FIRST CAUSE OF ACTION**

10 **(Equitable/Implied Indemnity)**

11 **(As to All Cross-Defendants, including ROES 1-50)**

12 12. Cross-Complainant refers to and incorporates herein by reference each and every
 13 preceding paragraph and all Causes of Action as though fully set forth herein.

14 13. In equity and good conscience, if Plaintiffs recover against Cross-Complainant,
 15 then Cross-Complainant is entitled to equitable indemnity, apportionment of liability, and
 16 contribution among, and from, the Cross-Defendants, and each of them, according to their
 17 respective fault, for the injuries and damages allegedly sustained by any and all Plaintiffs, if any,
 18 by way of sums paid by settlement, or in the alternative, any judgments rendered against
 19 Cross-Complainant in this action.

20 14. Cross-Complainant expressly denies the allegations of the Complaint and any
 21 wrongdoing on its part. Should Cross-Complainant nevertheless be found liable for any alleged
 22 wrongdoings with respect to Plaintiffs' allegations, the acts and/or omissions of
 23 Cross-Complainant was passive and secondary, while those of Cross-Defendants, and each of
 24 them, were active, primary and superseding. Thus, as a direct, proximate and foreseeable result of
 25 the wrongdoing of Cross-Defendants herein, and each of them, Cross-Complainant is entitled to
 26 total equitable indemnity from Cross-Defendants with respect to any and all liability adjudged
 27 against Cross-Complainant.

28 ///

1 15. As a direct, proximate and foreseeable result of the filing of the Complaint,
 2 Cross-Complainant has been compelled to incur attorneys' fees, court costs and the expense of this
 3 cross-action and Cross-Complainant will seek leave of court to amend its Cross-Complaint to set
 4 forth the amount of said damages when the same have been ascertained.

5 16. Should Plaintiffs recover any amount of damages against Cross-Complainant by
 6 way of judgment, settlement or otherwise, then Cross-Complainant by reason of the foregoing and
 7 in equity and good conscience, is entitled to an equitable apportionment of the liability of
 8 Cross-Defendants, and each of them, on a comparative fault basis and a judgment against
 9 Cross-Defendants, and each of them, under the doctrine of implied indemnity and in an amount
 10 equal to their respective liabilities as so apportioned.

11 **SECOND CAUSE OF ACTION**

12 **(Implied Contractual Indemnity)**

13 **(As to Cross-Defendants NETGAIN)**

14 17. Cross-Complainant refers to and incorporates herein by reference each and every
 15 paragraph of all Causes of Action herein as though fully set forth.

16 18. Cross-Complainant denies the allegations of Plaintiffs, and, without admitting the
 17 allegations contained therein, if it is found that Cross-Complainant is liable for any such damage
 18 to Plaintiffs or Cross-Defendants, then Cross-Complainant is informed and believes and thereon
 19 alleges that such damage is primarily and ultimately caused by the acts, breaches and/or omissions
 20 of Cross-Defendant NETGAIN whereas Cross-Complainant's acts, if any, were secondary, passive
 21 or derivative in nature.

22 19. Cross-Complainant is informed and believes and thereon alleges that
 23 Cross-Complainant entered into written and/or oral agreements with Cross-Defendant NETGAIN
 24 wherein Cross-Defendant NETGAIN agreed to provide computer services to Cross-Complainant,
 25 which is the subject of the action herein. Cross-Defendant NETGAIN further agreed to take all
 26 reasonable steps to ensure that non-public/confidential information of Cross-Complaint's
 27 consumers will not be disclosed.

28 ///

20. By reason of the foregoing, if Plaintiffs recover against Cross-Complainant, Cross-Complainant is entitled to indemnity from Cross-Defendant NETGAIN, for injuries and damages sustained by Plaintiffs, if any, for any sums paid by way of settlement, or in the alternative, any judgment rendered against Cross-Complainant in the action herein based upon the Complaint and any cause of action alleged therein.

21. Cross-Complainant is informed and believes and thereon alleges that Cross-Complainants entered into written and/or oral agreements with the NETGAIN in connection with the services which provides, among other things, for payment of costs and fees in defending any litigation arising with respect to the services which is the subject matter of this litigation.

22. Cross-Complainant has retained the services of WOOD, SMITH, HENNING & BERMAN LLP to defend the action herein, thereby incurring costs, consultants' fees, attorneys' fees and other litigation fees in the defense of this action and prosecution of this Cross-Complaint. Cross-Complainant will seek leave of this Court to amend this Cross-Complaint to show the amount of said costs and attorneys' fees when the same become known to Cross-Complainant.

THIRD CAUSE OF ACTION

(Breach of Written Contract)

(As to Cross-Defendants NETGAIN)

23. Cross-Complainant refers to and incorporates herein by reference each and every paragraph of all Causes of Action herein as though fully set forth.

24. Cross-Complainant is informed and believes and thereon alleges that Cross-Defendant NETGAIN entered into written agreements with Cross-Complainant, the terms of which shall be according to proof at time of trial.

25. Cross-Defendant NETGAIN, was required to indemnify Cross-Complainant with respect to the claims made and costs incurred on behalf of Cross-Complainant, in defending against the allegations set forth by Plaintiffs, as are more particularly described in their respective Cross-Complaint.

26. Cross-Complainant is informed and believes and thereon alleges that Cross-Defendant NETGAIN, entered into written agreements with Cross-Complainant and was to

WOOD, SMITH, HENNING & BERMAN LLP
 Attorneys at Law
 10960 WILSHIRE BOULEVARD, 18TH FLOOR
 LOS ANGELES, CALIFORNIA 90024-3804
 TELEPHONE 310-481-7600 ♦ FAX 310-481-7650

1 comply, with each and every term and condition.

2 27. Cross-Complainant is informed and believes and thereon alleges that the causes of
 3 action against Cross-Complainant claimed by Plaintiffs solely arise out of the Netgain Incident,
 4 which was a result of Cross-defendant NETGAIN's failure to take all reasonable steps to ensure
 5 that the non-public confidential information of Plaintiffs was not subject to unauthorized access
 6 and/or disclosure, pursuant to the agreement with Cross-Complainant; and Cross-Complainant
 7 herein is further informed and believes, and thereon alleges, that said damages were caused by
 8 Cross-Defendant NETGAIN who entered into a contract with Cross-Complainant to provide
 9 computer related services to Cross-Complainant and to take all reasonable steps to ensure that
 10 non-public/confidential information of Plaintiffs will not be disclosed in the performance of
 11 services provided; and are responsible for all acts and omissions of their agents and employees.

12 28. Cross-Complainant has performed all conditions, covenants and promises required
 13 by it in accordance with the terms and conditions of the aforementioned agreements.

14 29. Cross-Defendant NETGAIN has breached the aforementioned written contracts by
 15 failing to comply with each and every term of the contract.

16 30. As a result of Cross-Defendant NETGAIN breaching the aforementioned written
 17 contracts, Cross-Complainant has been damaged in an amount according to proof at the time of
 18 trial.

19 31. Cross-Complainant is informed and believes and thereon alleges that the contracts
 20 provide, that Cross-Defendant NETGAIN, among other things, was to comply with each and
 21 every term and condition.

22 32. Cross-Complainant has retained the services of WOOD, SMITH, HENNING &
 23 BERMAN LLP to defend the action herein, thereby incurring costs, consultants' fees, attorneys'
 24 fees and other litigation fees in the defense of this action and prosecution of this Cross-Complaint.
 25 Cross-Complainant will seek leave of this court to amend this Cross-Complaint to show the
 26 amount of said costs and attorneys' fees when the same become known to Cross-Complainant.

27 ///

28 ///

FOURTH CAUSE OF ACTION

(Contribution)

(As to NETGAIN, including ROES 1-50)

33. Cross-Complainant refers to and incorporates herein by reference each and every paragraph of all Causes of Action, as though fully set forth.

34. If Cross-Complainant is held liable in this action, then under the doctrine of indemnity for comparative fault, Cross-Complainant is entitled to contribution and/or indemnification on the basis that the Cross-Defendants NETGAIN, including All ROES, and each of them, should be required to share liability with Cross-Complainant pro rata, on the basis of the relative fault of each party whose tortuous conduct caused or contributed to the damages, if any there be. Further, Cross-Complainant is entitled to be reimbursed for attorneys' fees and expenses in defending said action, and that Cross-Complainant should have a pro rata carry-over judgment against the foregoing Cross-Defendants, and each of them.

FIFTH CAUSE OF ACTION

(Apportionment of Fault)

(As to NETGAIN, including ROES 1-50)

35. Cross-Complainant refers to and incorporates herein by reference each and every paragraph of all Causes of Action, as though fully set forth.

36. Cross-Complainant alleges that Cross-Defendants, and each of them, were responsible, in whole or in part, for the injuries, if any, suffered by Plaintiffs.

37. If Cross-Complainant is judged liable, then Cross-Defendants, and each of them, must be required to pay a share of Plaintiffs' judgment which is in proportion to the comparative negligence of Cross-Defendants in causing the Plaintiffs' damages and must reimburse Cross Complainant for any payments Cross-Complainant made to the Plaintiffs in excess of Cross Complainants' proportional share of all Cross-Defendants' negligence.

///

///

///

WOOD, SMITH, HENNING & BERMAN LLP
Attorneys at Law
10960 WILSHIRE BOULEVARD, 18TH FLOOR
LOS ANGELES, CALIFORNIA 90024-3804
TELEPHONE 310-481-7600 ♦ FAX 310-481-7650

SIXTH CAUSE OF ACTION

(Declaratory Relief)

(As to NETGAIN, including ROES 1-50)

38. Cross-Complainant refers to and incorporates herein by reference each and every paragraph of all Causes of Action, as though fully set forth.

39. An actual controversy has arisen and now exists between Cross-Complainant and Cross-Defendant NETGAIN concerning their respective rights and duties in that Cross-Complainant contends that it is entitled to an offset of alleged damages and that Cross-Defendants are obligated to indemnify Cross-Complainant against liability in an amount proportionate to the respective fault of Cross-Defendants in causing damages as alleged in the main Complaint and the Cross-Complaints. Cross-Complainant is informed and believes and thereon alleges that Cross-Defendants dispute these contentions and contend that they are under no obligation to indemnify Cross-Complainant, or any other party to this action.

40. Cross-Complainant desires a judicial determination of its rights and duties and a declaration that it be indemnified for any portion of the recovery of any other party to this action against the Plaintiffs to the extent that Cross-Complainant is found to be at fault in causing the damages alleged in the Plaintiffs' Complaints in this action.

41. Such a declaration is necessary and appropriate at this time in order that Cross-Complainant may ascertain its rights and duties. In the absence of such a determination, Cross-Complainant will be forced to defend the main action herein, handicapped by the uncertainty as to their rights of indemnification from Cross-Defendants, and each of them.

WHEREFORE, Cross-Complainant, prays for judgment against Cross-Defendants, and each of them, as follows:

FIRST CAUSE OF ACTION:

That Cross-Complainant be entitled to equitable/implied indemnity from all Cross-Defendants, and each of them;

SECOND CAUSE OF ACTION:

That Cross-Complainant be entitled to implied contractual indemnity from Cross-

1 Defendant NETGAIN, and each of them;

2 **THIRD CAUSE OF ACTION:**

3 That Cross-Complainant be entitled to breach of written contract from Cross-Defendant
4 NETGAIN, and each of them;

5 **FOURTH CAUSE OF ACTION:**

6 That Cross-Complainant be entitled to contribution from all Cross-Defendants and each of
7 them;

8 **FIFTH CAUSE OF ACTION:**

9 That Cross-Complainant be entitled to apportionment of fault from all Cross-Defendants,
10 and each of them; and

11 **SIXTH CAUSE OF ACTION:**

12 For judgment against Cross-Defendants, and each of them, declaring that Cross-
13 Complainant is entitled to a judgment of several liability separate, distinct and apart from any joint
14 and/or several liability which may be rendered against any one of the Cross-Defendants, and each
15 of them.

16 **AS TO ALL CAUSES OF ACTION:**

- 17 1. For costs of suit incurred herein, including, but not limited to, costs of investigation
18 incurred in the prosecution of this Cross-Complaint;
- 19 2. For attorneys' fees incurred herein in the defense of the this Cross-Complaint and
20 in the prosecution of this Cross-Complaint; and
- 21 3. For such other and further relief as the Court may deem just and proper.

22 DATED: November 29, 2021

23
24 WOOD, SMITH, HENNING & BERMAN LLP

25
26 By: 

27 NATHAN A. GUEST

28 Attorneys for Cross-Defendant, LIFELONG MEDICAL
CARE, a California corporation

PROOF OF SERVICE

Margolies v. Lifelong Medical Care
Case No. RG21113030

I am employed in the County of Los Angeles, State of California. I am over the age of eighteen years and not a party to the within action. My business address is 10960 Wilshire Boulevard, 18th Floor, Los Angeles, CA 90024-3804.

On November 29, 2021, I served the following document(s) described as **CROSS-COMPLAINT OF LIFELONG MEDICAL CARE** on the interested parties in this action as follows:

SEE ATTACHED SERVICE LIST

BY E-MAIL OR ELECTRONIC TRANSMISSION: Based on a court order or an agreement of the parties to accept service by e-mail or electronic transmission, I caused the document(s) to be sent from e-mail address jduggans@wshbmail.com to the persons at the electronic notification address listed in the service list. I did not receive, within a reasonable time after the transmission, any electronic message or other indication that the transmission was not successful.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed on November 29, 2021, at Los Angeles, California.

Jamila Duggans

Jamila L. Duggans

WOOD, SMITH, HENNING & BERMAN LLP
Attorneys at Law
10960 WILSHIRE BOULEVARD, 18TH FLOOR
LOS ANGELES, CALIFORNIA 90024-3804
TELEPHONE 310-481-7600 ♦ FAX 310-481-7650

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

SERVICE LIST
Margolies v. Lifelong Medical Care
Case No. RG21113030

Abbas Kazerounian, Esq.
Mona Amini, Esq.
Kazerouni Law Group, APC
245 Fischer Ave.
Unit D1
Costa Mesa, CA 92626
Tel: (800) 400-6808 / Fax: (800) 520-5523
E-mail: ak@kazlg.com
mona@kazlg.com
Attorneys for Plaintiff NOEM
MARGOLIES; and the Proposed Class

WOOD, SMITH, HENNING & BERMAN LLP
Attorneys at Law
10960 WILSHIRE BOULEVARD, 18TH FLOOR
LOS ANGELES, CALIFORNIA 90024-3804
TELEPHONE 310-481-7600 ♦ FAX 310-481-7650

EXHIBIT "4"

ELECTRONICALLY FILED

Superior Court of California,
County of Alameda

12/06/2021 at 04:50:04 PM

By: Curtiyah Garter, Deputy Clerk

1 Nathan A. Guest (State Bar No. 330167)
nguest@wshblaw.com
2 **WOOD, SMITH, HENNING & BERMAN LLP**
10960 Wilshire Boulevard, 18th Floor
3 Los Angeles, California 90024-3804
Phone: 310-481-7600 ♦ Fax: 310-481-7650
4

Attorneys for Defendant, LIFELONG MEDICAL CARE, a California corporation
5
6

7 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
8 **FOR THE COUNTY OF ALAMEDA – COMPLEX CIVIL**
9

10 NOEM MARGOLIES, individually and on
behalf of all others similarly situated,

11 Plaintiffs,

12 v.

13 LIFELONG MEDICAL CARE, a California
14 corporation; and DOES 1-50, inclusive,

15 Defendant(s).
16
17

RG21113030

**DEFENDANT LIFELONG MEDICAL
CARE'S ANSWER TO PLAINTIFFS'
COMPLAINT**

DEMAND FOR JURY TRIAL

[Assigned for All Purposes to Judge Evelio M. Grillo, Dept.
21]

Action Filed: 9/17/21

Trial Date: None Set

18
19 Defendant Lifelong Medical Care ("Defendant") hereby answers the Complaint filed by
20 Plaintiff, Noem Margolies, on behalf of himself and all others similarly situated ("Plaintiffs"):

21 **GENERAL AND SPECIFIC DENIALS**

22 Pursuant to the provisions of California *Code of Civil Procedure* section 431.30(d),
23 Defendant denies, generally and specifically, each and every allegation contained in the
24 Complaint, and further denies that Plaintiffs have been damaged in the amount or amounts alleged
25 therein, or in any other amount, or at all, by reason of any act or omission on the part of
26 Defendant, or by any act or omission by any agent or employee of Defendant. Defendant further
27 denies, generally and specifically, that Plaintiffs are entitled to any relief whatsoever.
28

FIRST AFFIRMATIVE DEFENSE

(Failure to State a Cause of Action)

1. As a separate and affirmative defense to the Complaint, Defendant is informed and believes, and thereon alleges, that Plaintiffs are barred from recovery herein by reason of the fact that the Complaint, and each and every cause of action thereof, fails to state facts sufficient to constitute a cause of action against Defendant.

SECOND AFFIRMATIVE DEFENSE

(Lack of Standing)

2. As a separate and affirmative defense to the Complaint, Defendant alleges that the Plaintiffs, as alleged in the Complaint, do not have standing to bring one or more of their causes of action.

THIRD AFFIRMATIVE DEFENSE

(Failure to Mitigate)

3. As a separate and affirmative defense to the Complaint, Defendant is informed and believes, and thereon alleges, that Plaintiffs are barred from recovery under any and all causes of action alleged in the Complaint by reason of their failure and refusal to mitigate their damages, if any, incurred as a result of any and all matters alleged in the Complaint, despite their ability to do so by the exercise of reasonable effort.

FOURTH AFFIRMATIVE DEFENSE

(Defendant's Cure – California Civil Code § 1798.150(a)(1))

4. As a separate and affirmative defense to the Complaint, Defendant alleges that it cured any alleged violation of the California Consumer Privacy Act pursuant to California Civil Code section 1798.150(a)(1) and, therefore, Plaintiffs are barred from seeking statutory damages.

FIFTH AFFIRMATIVE DEFENSE

(Comparative Negligence)

5. As a separate and affirmative defense to the Complaint, Defendant alleges that without admitting that Plaintiffs suffered any damage or damages, Plaintiffs' right of recovery, if any, is barred or diminished because the damages sustained by Plaintiffs, if any, were proximately

WOOD, SMITH, HENNING & BERMAN LLP
Attorneys at Law
10960 WILSHIRE BOULEVARD, 18TH FLOOR
LOS ANGELES, CALIFORNIA 90024-3804
TELEPHONE 310-481-7600 ♦ FAX 310-481-7650

1 caused by the negligence of others not under the control of Defendant including but not limited to,
 2 Plaintiffs and/or other persons, which negligence bars or diminishes the recovery, if any, of
 3 Plaintiffs against Defendant.

4 **SIXTH AFFIRMATIVE DEFENSE**

5 **(Comparative Fault)**

6 6. As a separate and affirmative defense to the Complaint, Defendant alleges that
 7 without admitting that Plaintiffs suffered any damage or damages, Plaintiffs' right of recovery, if
 8 any, is barred or diminished because the damages sustained by Plaintiffs, if any, were proximately
 9 caused by the fault of others not under the control of Defendant, including but not limited to,
 10 Plaintiffs and/or other persons, which faults bars or diminishes the recovery, if any, of Plaintiffs
 11 against Defendant.

12 **SEVENTH AFFIRMATIVE DEFENSE**

13 **(Reimbursement)**

14 7. As a separate and affirmative defense to the Complaint, Defendant alleges that any
 15 reimbursement, from whatever source, to Plaintiffs of the alleged damages must be applied against
 16 any liability of Defendant.

17 **EIGHTH AFFIRMATIVE DEFENSE**

18 **(Statute of Limitations)**

19 8. As a separate and affirmative defense to the Complaint, Defendant alleges that
 20 Plaintiffs' purported causes of action against Defendant are barred by the applicable statute of
 21 limitations.

22 **NINTH AFFIRMATIVE DEFENSE**

23 **(Waiver)**

24 9. As a separate and affirmative defense to the Complaint, Defendant is informed and
 25 believes, and thereon alleges, that Plaintiffs engaged in conduct and activities sufficient to
 26 constitute a waiver of any alleged breach of duty, negligence, act, omission or any other conduct,
 27 if any, as set forth in the Complaint.
 28

WOOD, SMITH, HENNING & BERMAN LLP
 Attorneys at Law
 10960 WILSHIRE BOULEVARD, 18TH FLOOR
 LOS ANGELES, CALIFORNIA 90024-3804
 TELEPHONE 310-481-7600 ♦ FAX 310-481-7650

TENTH AFFIRMATIVE DEFENSE**(Unjust Enrichment)**

10. As a separate and affirmative defense to the Complaint, Defendant is informed and believes, and thereon alleges, that payment of money to Plaintiffs for alleged violations or conduct which are the subject of the Complaint would constitute unjust enrichment.

ELEVENTH AFFIRMATIVE DEFENSE**(No Damages)**

11. As a separate and affirmative defense to the Complaint, Defendant is informed and believes, and thereon alleges, that Plaintiffs have suffered no cognizable damage as a result of any and all of the matters alleged in the Complaint.

TWELFTH AFFIRMATIVE DEFENSE**(Contribution)**

12. As a separate and affirmative defense to the Complaint, Defendant is informed and believes, and thereon alleges, that without admitting that Plaintiffs suffered any damage or damages, Defendant alleges that in the event Defendant is found liable to Plaintiffs, which liability is expressly denied, and any other parties, persons, or entities are likewise held liable to Plaintiffs, Defendant is entitled to a percentage reduction of their liability, reflecting the liability of such other parties, persons, or entities, in accordance with the principles of equitable indemnity and comparative contribution

THIRTEENTH AFFIRMATIVE DEFENSE**(Apportionment of Fault)**

13. As a separate and affirmative defense to the Complaint, Defendant is informed and believes, and thereon alleges, that without admitting that Plaintiffs suffered any damage or damages, Defendant alleges that Plaintiffs' right of recovery, if any, under all causes of action, is barred or diminished because Plaintiffs and/or other persons were negligent or otherwise at fault with respect to the matters set forth in the Complaint, thus, in the event of a settlement, judgment or other resolution in favor of Plaintiffs, Defendant requests that an apportionment of negligence or fault be made among all parties and other persons and further requests that a judgment or

1 declaration of partial or total indemnification and/or contribution be issued in accord with the
2 apportionment of negligence or fault

3 **FOURTEENTH AFFIRMATIVE DEFENSE**

4 **(Due Care)**

5 14. As a separate and affirmative defense to the Complaint, Defendant alleges that at
6 all relevant times, Defendant acted with due care and in accordance with all statutory and
7 regulatory requirements.

8 **FIFTEENTH AFFIRMATIVE DEFENSE**

9 **(Causation)**

10 15. As a separate and affirmative defense to the Complaint, Defendant is informed and
11 believes, and thereon alleges, that it did not affirmatively contribute to any of the injuries or
12 damages of which Plaintiffs complain.

13 **SIXTEENTH AFFIRMATIVE DEFENSE**

14 **(Proximate Cause)**

15 16. As a separate and affirmative defense to the Complaint, Defendant is informed and
16 believes, and thereon alleges, that Plaintiffs' alleged losses or damages, if any, were not
17 proximately caused or contributed to by any acts or omissions of Defendant.

18 **SEVENTEENTH AFFIRMATIVE DEFENSE**

19 **(Superseding and Intervening Act)**

20 17. As a separate and affirmative defense to the Complaint, Defendant is informed and
21 believes, and thereon alleges, that the injuries and damages sustained by Plaintiffs, if any, were
22 proximately caused by the intervening and superseding actions of others, which intervening and
23 superseding actions bar and/or diminish Plaintiffs' recovery, if any, against Defendant, or any of
24 them.

25 **EIGHTEENTH AFFIRMATIVE DEFENSE**

26 **(Collateral Source Rule)**

27 18. As a separate and affirmative defense to the Complaint, Defendant is informed and
28 believes, and thereon alleges, that Plaintiffs' award of damages, if any, must be reduced by the

WOOD, SMITH, HENNING & BERMAN LLP
Attorneys at Law
10960 WILSHIRE BOULEVARD, 18TH FLOOR
LOS ANGELES, CALIFORNIA 90024-3804
TELEPHONE 310-481-7600 ♦ FAX 310-481-7650

1 application of the collateral source rule.

2 **NINETEENTH AFFIRMATIVE DEFENSE**

3 **(Set Off)**

4 19. As a separate and affirmative defense to the Complaint, Defendant is informed and
5 believes, and thereon alleges, that it is entitled to a contractual and/or statutory set-off and/or
6 offset against any damages or claims recovered by Plaintiffs, if any, for Defendant's alleged
7 wrongful acts alleged by Plaintiffs in the Complaint.

8 **TWENTIETH AFFIRMATIVE DEFENSE**

9 **(Right to Add Other Affirmative Defenses)**

10 20. As a separate and affirmative defense to the Complaint, Defendant reserves the
11 right to allege further affirmative defenses as they become known through the course of discovery.
12 No defense is being knowingly or intentionally waived.

13 **PRAYER FOR RELIEF**

14 WHEREFORE, Defendant prays for judgment as follows:

- 15 1. That Plaintiffs take nothing by way of the Complaint;
16 2. That judgment be entered against Plaintiffs and in favor of Defendant on all causes
17 of action;
18 3. That Defendant be awarded attorneys' fees and costs of suit incurred herein; and
19 4. That Defendant be awarded such other and further relief as the Court may deem
20 just and proper.

21 **DEMAND FOR JURY TRIAL**

22 Defendant hereby demands a trial by jury in the above-entitled matter.

23 DATED: December 6, 2021

WOOD, SMITH, HENNING & BERMAN LLP

24
25 By: 

26 NATHAN A. GUEST

27 Attorneys for Defendant, LIFELONG MEDICAL
28 CARE, a California corporation

PROOF OF SERVICE

Margolies v. Lifelong Medical Care
Case No. RG21113030

I am employed in the County of Los Angeles, State of California. I am over the age of eighteen years and not a party to the within action. My business address is 10960 Wilshire Boulevard, 18th Floor, Los Angeles, CA 90024-3804.

On December 6, 2021, I served the following document(s) described as **DEFENDANT LIFELONG MEDICAL CARE'S ANSWER TO PLAINTIFFS' COMPLAINT** on the interested parties in this action as follows:

SEE ATTACHED SERVICE LIST

BY E-MAIL OR ELECTRONIC TRANSMISSION: Based on a court order or an agreement of the parties to accept service by e-mail or electronic transmission, I caused the document(s) to be sent from e-mail address jduggans@wshbmail.com to the persons at the electronic notification address listed in the service list. I did not receive, within a reasonable time after the transmission, any electronic message or other indication that the transmission was not successful.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed on December 6, 2021, at Los Angeles, California.

Jamila Duggans

Jamila L. Duggans

WOOD, SMITH, HENNING & BERMAN LLP
Attorneys at Law
10960 WILSHIRE BOULEVARD, 18TH FLOOR
LOS ANGELES, CALIFORNIA 90024-3804
TELEPHONE 310-481-7600 ♦ FAX 310-481-7650

WOOD, SMITH, HENNING & BERMAN LLP
Attorneys at Law
10960 WILSHIRE BOULEVARD, 18TH FLOOR
LOS ANGELES, CALIFORNIA 90024-3804
TELEPHONE 310-481-7600 ♦ FAX 310-481-7650

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

SERVICE LIST
Margolies v. Lifelong Medical Care
Case No. RG21113030

Abbas Kazerounian, Esq.
Mona Amini, Esq.
Kazerouni Law Group, APC
245 Fischer Ave.
Unit D1
Costa Mesa, CA 92626
Tel: (800) 400-6808 / Fax: (800) 520-5523
E-mail: ak@kazlg.com
mona@kazlg.com
Attorneys for Plaintiff NOEM
MARGOLIES; and the Proposed Class

PROOF OF SERVICE

Cowan, et al. v. Lifelong Medical Care
Case No. 21CV000478

I am employed in the County of Los Angeles, State of California. I am over the age of eighteen years and not a party to the within action. My business address is 10960 Wilshire Boulevard, 18th Floor, Los Angeles, CA 90024-3804.

On December 29, 2021, I served the following document(s) described as **NOTICE OF REMOVAL OF ACTION UNDER 28 U.S.C.A. § 1332(d)** on the interested parties in this action as follows:

SEE ATTACHED SERVICE LIST

BY MAIL: I placed true copies of the foregoing document(s) enclosed in sealed envelopes addressed as shown on the Service List. I am “readily familiar” with Wood, Smith, Henning & Berman’s practice for collecting and processing correspondence for mailing with the United States Postal Service. Under that practice, it would be deposited with the United States Postal Service that same day in the ordinary course of business. Such envelope(s) were placed for collection and mailing with postage thereon fully prepaid at Los Angeles, California, on that same day following ordinary business practices.

BY E-MAIL OR ELECTRONIC TRANSMISSION: Based on a court order or an agreement of the parties to accept service by e-mail or electronic transmission, I caused the document(s) to be sent from e-mail address jduggans@wshbmail.com to the persons at the electronic notification address listed in the service list. I did not receive, within a reasonable time after the transmission, any electronic message or other indication that the transmission was not successful.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed on December 29, 2021, at Los Angeles, California.

Jamila Duggans

 Jamila L. Duggans

WOOD, SMITH, HENNING & BERMAN LLP
 Attorneys at Law
 10960 WILSHIRE BOULEVARD, 18TH FLOOR
 LOS ANGELES, CALIFORNIA 90024-3804
 TELEPHONE 310-481-7600 ♦ FAX 310-481-7650

SERVICE LIST
Margolies v. Lifelong Medical Care
Case No. RG21113030

VIA E-MAIL:

Abbas Kazerounian, Esq.
Mona Amini, Esq.
Kazerouni Law Group, APC
245 Fischer Ave.
Unit D1
Costa Mesa, CA 92626
Tel: (800) 400-6808 / Fax: (800) 520-5523
E-mail: ak@kazlg.com
mona@kazlg.com
Attorneys for Plaintiff NOEM
MARGOLIES; and the Proposed Class

VIA U.S. MAIL:

NETGAIN TECHNOLOGY, INC
ATTN: SCOTT WARZECHA
(Registered Agent)

26 6th Avenue N. #360
St. Cloud, MN 56303

720 W St. Germain Street
St. Cloud, MN 56301

NETGAIN TECHNOLOGY, LLC
ATTN: SCOTT WARZECHA
(Registered Agent)

26 6th Avenue N. #360
St. Cloud, MN 56303

720 W St. Germain Street
St. Cloud, MN 56301

NETGAIN TECHNOLOGY, INC.
ATTN: TODD DEWENTER
(Registered Agent)

912 W. St. Germain Street
Floor B
St. Cloud, MN 56303

WOOD, SMITH, HENNING & BERMAN LLP
Attorneys at Law
10960 WILSHIRE BOULEVARD, 18TH FLOOR
LOS ANGELES, CALIFORNIA 90024-3804
TELEPHONE 310-481-7600 ♦ FAX 310-481-7650